

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-033727
(43)Date of publication of application : 31.01.2002

(51)Int.Cl. H04L 9/10
G06F 12/00
G06F 12/14
H04L 9/08
H04L 9/32

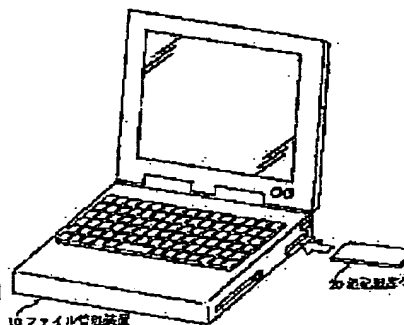
(21)Application number : 2001-137650 (71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(22)Date of filing : 08.05.2001 (72)Inventor : MATSUZAKI NATSUME
EMURA SATOSHI
INAGAKI SATORU

(30)Priority
Priority number : 2000138642 Priority date : 11.05.2000 Priority country : JP

(54) FILE MANAGEMENT SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a file management system that can surely decode encrypted information, when a user forgets a password.
SOLUTION: A password registration section 100 uses a password, to encrypt key information and to store an encrypted key. A file encryption section 200 uses the key information to encrypt a file key and to generate an encrypted file key, uses the file key to encrypt a plain text and generates an encrypted text to store the encrypted file key and the encrypt text. A file decoding section 300 decodes the encrypted file key, by using the key information to obtain a file key, when using the key information. When using the password, the password is received, the encryption key is decoded by the password to obtain the key information, the file key is decoded by using the encrypted file key to obtain the file key. Then the encrypted text is decoded by the file key.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

BEST AVAILABLE COPY

BEST AVAILABLE COPY

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-33727

(P2002-33727A)

(43) 公開日 平成14年1月31日 (2002.1.31)

(51) Int.Cl. ⁷	識別記号	F I	テラコード (参考)
H 0 4 L 9/10		G 0 6 F 12/00	5 3 7 H 5 B 0 1 7
G 0 6 F 12/00	5 3 7	12/14	3 2 0 B 5 B 0 8 2
12/14	3 2 0		3 2 0 C 5 J 1 0 4
		H 0 4 L 9/00	6 2 1 A
H 0 4 L 9/08			6 7 3 C

審査請求 未請求 請求項の数37 O L (全 24 頁) 最終頁に続く

(21) 出願番号 特願2001-137650 (P2001-137650)

(22) 出願日 平成13年5月8日 (2001.5.8)

(31) 優先権主張番号 特願2000-198642 (P2000-198642)

(32) 優先日 平成12年5月11日 (2000.5.11)

(33) 優先権主張国 日本 (J P)

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 松崎 なつめ

大阪府門真市大字門真1006番地 松下電器

産業 株式会社内

(72) 発明者 江村 里志

大阪府門真市大字門真1006番地 松下電器

産業 株式会社内

(74) 代理人 100090446

弁理士 中島 司朗

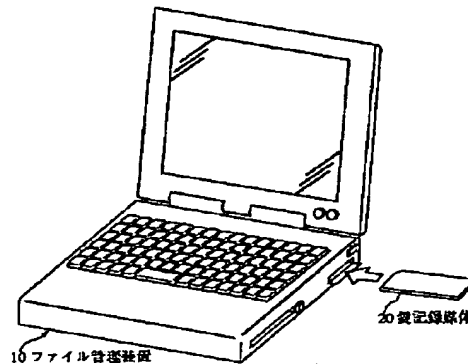
最終頁に続く

(54) 【発明の名称】 ファイル管理装置

(57) 【要約】

【課題】 利用者がパスワードを忘れたとき、暗号化された情報が確実に復号できるファイル管理装置を提供する。

【解決手段】 パスワード登録部100はパスワードを用いて鍵情報を暗号化し暗号化鍵を保存する。ファイル暗号部200は鍵情報を用いてファイル鍵を暗号化して暗号化ファイル鍵を生成しファイル鍵を用いて平文を暗号化して暗号文を生成し暗号化ファイル鍵と暗号文とを保存する。鍵情報を用いるときファイル復号部300は暗号化ファイル鍵を鍵情報を用いて復号してファイル鍵を求める。パスワードを用いるときパスワードを受け付け暗号化鍵をパスワードで復号して鍵情報求め鍵情報で暗号化ファイル鍵を復号してファイル鍵を求める。次にファイル鍵で暗号文を復号する。



(2) 特開 2002-33727

【特許請求の範囲】

【請求項 1】 平文を暗号化して記憶し、復号するファイル管理装置であって、

鍵情報を予め記憶している鍵記録媒体と、

入力されるパスワードを用いて前記鍵情報を暗号化して暗号化鍵を生成する登録手段と、

前記鍵記録媒体に記憶されている鍵情報に基づいて、平文を暗号化して暗号文を生成する暗号手段と、

前記鍵記録媒体から鍵情報を読み出すか、又は入力されるパスワードを用いて前記暗号化鍵を復号して鍵情報を生成するかを切り換える切換手段と、

前記鍵情報に基づいて暗号文を復号する復号手段とを備えることを特徴とするファイル管理装置。

【請求項 2】 前記ファイル管理装置は、さらにメモリ部を有し、

前記登録手段は、パスワードの入力を受け付け、前記パスワードを用いて前記鍵情報を暗号化して暗号化鍵を生成し、生成した前記暗号化鍵をメモリ部に書き込み、

前記暗号手段は、ファイル鍵を用いて平文を暗号化して暗号文を生成し、前記鍵情報を用いて前記ファイル鍵を暗号化して暗号化ファイル鍵を生成し、前記暗号文と前記暗号化ファイル鍵とを対応付けてメモリ部に書き込み、

前記切換手段は、前記パスワードの入力を受け付け、前記パスワードを用いて前記暗号化鍵を復号して鍵情報を生成する第 1 鍵獲得手段と、第 2 タイプの入力を受け付けた場合に、前記鍵記録媒体から鍵情報を読み出す第 2 鍵獲得手段とを含み、前記切換手段は、前記第 1 及び第 2 鍵獲得手段のいずれかにより鍵情報を獲得し、前記復号手段は、前記鍵情報を用いて前記暗号化ファイル鍵を復号してファイル鍵を生成し、前記ファイル鍵を用いて前記暗号文を復号して復号文を生成することを特徴とする請求項 1 に記載のファイル管理装置。

【請求項 3】 前記登録手段は、さらに利用者を識別する利用者識別子の入力を受け付け、前記利用者識別子と対応付けて前記暗号化鍵をメモリ部に書き込み、

前記第 1 鍵獲得手段は、さらに前記利用者識別子の入力を受け付け、前記利用者識別子に対応付けられた前記暗号化鍵を復号することを特徴とする請求項 2 に記載のファイル管理装置。

【請求項 4】 前記登録手段は、さらに前記鍵情報又は認証情報を前記暗号化鍵と対応付けてメモリ部に書き込み、

前記暗号手段は、さらに前記暗号化鍵、前記鍵情報又は認証情報を前記暗号文と対応付けてメモリ部に書き込み、

前記第 1 鍵獲得手段は、さらに前記認証情報が対応付けられた前記暗号化鍵を復号する場合に、前記認証情報を用いて前記暗号化鍵の改変の有無を検証し、

前記復号手段は、さらに前記認証情報が対応付けられた

前記暗号文を復号する場合に、前記認証情報を用いて前記暗号文の改変の有無を検証することを特徴とする請求項 2 に記載のファイル管理装置。

【請求項 5】 前記登録手段は、前記暗号化鍵を可搬型記録媒体であるメモリ部に書き込み、

前記第 1 鍵獲得手段は、前記可搬型記録媒体であるメモリ部に書き込まれている前記暗号化鍵を復号することを特徴とする請求項 2 に記載のファイル管理装置。

【請求項 6】 前記ファイル管理装置は、さらに、メモリ部に書き込まれている前記暗号化鍵を削除する削除手段を含むことを特徴とする請求項 2 に記載のファイル管理装置。

【請求項 7】 前記ファイル管理装置は、さらに、メモリ部に書き込まれている前記暗号化鍵を削除する削除手段を含み、

前記登録手段は、さらに、新パスワードの入力を受け付け、前記新パスワードを用いて前記鍵情報を暗号化して新暗号化鍵を生成し、生成した前記新暗号化鍵をメモリ部に書き込むことを特徴とする請求項 2 に記載のファイル管理装置。

【請求項 8】 前記鍵記録媒体は、前記鍵情報に代えて、新鍵情報を予め記憶しており、

前記登録手段は、さらに前記パスワードの入力を受け付け、前記パスワードを用いて前記暗号化鍵を復号して鍵情報を生成し、

前記暗号手段は、さらに前記鍵情報を用いて前記暗号化ファイル鍵を復号してファイル鍵を生成し、前記新鍵情報を用いて前記ファイル鍵を暗号化して新暗号化ファイル鍵を生成し、前記暗号化ファイル鍵に代えて前記新暗号化ファイル鍵をメモリ部に書き込み、

前記登録手段は、さらに前記パスワードを用いて前記新鍵情報を暗号化して新暗号化鍵を生成し、前記暗号化鍵に代えて生成した前記新暗号化鍵をメモリ部に書き込むことを特徴とする請求項 2 に記載のファイル管理装置。

【請求項 9】 前記登録手段は、さらに利用者を識別する利用者識別子の入力を受け付け、

前記暗号手段は、さらに前記利用者識別子を前記暗号文及び前記暗号化ファイル鍵に対応付けてメモリ部に書き込み、

前記暗号手段は、メモリ部内において前記利用者識別子に対応づけられた前記暗号化ファイル鍵を検索し、検索された前記暗号化ファイル鍵からファイル鍵を生成することを特徴とする請求項 8 に記載のファイル管理装置。

【請求項 10】 前記暗号手段は、さらに暗号化を示す暗号化情報を前記暗号文及び前記暗号化ファイル鍵に対応付けてメモリ部に書き込み、

前記暗号手段は、メモリ部内において暗号化情報に対応づけられた前記暗号化ファイル鍵を検索し、検索された前記暗号化ファイル鍵からファイル鍵を生成することを特徴とする請求項 8 に記載のファイル管理装置。

(3) 特開 2002-33727

3

【請求項 11】 前記登録手段は、さらに利用者を識別する利用者識別子の入力を受け付け、

前記暗号手段は、さらに前記利用者識別子と、前記暗号文及び前記暗号化ファイル鍵を識別するファイル識別子とを対応付けて一括ファイルとしてメモリ部に書き込み、

前記暗号手段は、前記一括ファイルから前記利用者識別子に対応づけられたファイル識別子を抽出し、抽出されたファイル識別子により識別される前記暗号化ファイル鍵を特定し、特定された前記暗号化ファイル鍵からファイル鍵を生成することを特徴とする請求項 8 に記載のファイル管理装置。

【請求項 12】 前記暗号手段は、さらに暗号化を示す暗号化情報と、前記暗号文及び前記暗号化ファイル鍵を識別するファイル識別子とを対応付けて一括ファイルとしてメモリ部に書き込み、

前記暗号手段は、前記一括ファイルから前記暗号化情報に対応づけられたファイル識別子を抽出し、抽出されたファイル識別子により識別される前記暗号化ファイル鍵を特定し、特定された前記暗号化ファイル鍵からファイル鍵を生成することを特徴とする請求項 8 に記載のファイル管理装置。

【請求項 13】 前記暗号手段は、さらに前記暗号化鍵を前記暗号文及び前記暗号化ファイル鍵に対応付けてメモリ部に書き込み、

前記第 1 鍵獲得手段は、前記暗号文及び前記暗号化ファイル鍵と対応付けて記憶されている前記暗号化鍵を復号することを特徴とする請求項 2 に記載のファイル管理装置。

【請求項 14】 前記暗号手段は、さらに、暗号化鍵と暗号文とを対応付けてメモリ部に書き込むか否かを示す指示の入力を受け付け、前記指示が対応付けて書き込むことを示す場合に、前記暗号化鍵を前記暗号文と対応付けてメモリ部に書き込むことを特徴とする請求項 13 に記載のファイル管理装置。

【請求項 15】 前記登録手段は、生成した前記暗号化鍵を、メモリ部に代えて、前記記録媒体に書き込むことを特徴とする請求項 13 に記載のファイル管理装置。

【請求項 16】 平文を暗号化してメモリ部に記憶するファイル暗号装置であって、

鍵情報を予め記憶している鍵記録媒体と、パスワードの入力を受け付け、前記パスワードを用いて前記鍵情報を暗号化して暗号化鍵を生成し、生成した前記暗号化鍵をメモリ部に書き込む登録手段と、

ファイル鍵を用いて平文を暗号化して暗号文を生成し、前記鍵情報を用いて前記ファイル鍵を暗号化して暗号化ファイル鍵を生成し、前記暗号文と前記暗号化ファイル鍵とを対応付けてメモリ部に書き込む暗号手段とを備えることを特徴とするファイル暗号装置。

【請求項 17】 請求項 16 に記載のファイル暗号装置

4

により生成された前記暗号文と前記暗号化ファイル鍵とが対応付けてメモリ部に記憶されており、前記暗号文を復号するファイル復号装置であって、

鍵情報を予め記憶している鍵記録媒体と、

前記パスワードの入力を受け付け、前記パスワードを用いて前記暗号化鍵を復号して鍵情報を生成する第 1 鍵獲得手段と、前記鍵記録媒体から鍵情報を読み出す第 2 鍵獲得手段とを含み、前記第 1 及び第 2 鍵獲得手段のいずれかにより鍵情報を獲得する切換手段と、

10 前記鍵情報を用いて前記暗号化ファイル鍵を復号してファイル鍵を生成し、前記ファイル鍵を用いて前記暗号文を復号して復号文を生成する復号手段とを備えることを特徴とするファイル復号装置。

【請求項 18】 平文を暗号化して記憶し、復号するファイル管理装置であって、

鍵情報を予め記憶している鍵記録媒体と、

前記鍵情報を用いて入力されるパスワードを暗号化する登録手段と、

ファイル鍵を用いて平文を暗号化して暗号文を生成し、

20 前記鍵情報と前記暗号化されたパスワードを復号して得られたパスワードとに基づいて、ファイル鍵を暗号化してそれぞれ暗号化ファイル鍵を生成する暗号手段と、前記鍵情報に基づいて暗号化ファイル鍵を復号するか、又は入力されたパスワードに基づいて暗号化ファイル鍵を復号するかを切り換えて、ファイル鍵を生成する切換手段と、

前記ファイル鍵に基づいて暗号文を復号する復号手段とを備えることを特徴とするファイル管理装置。

【請求項 19】 前記ファイル管理装置は、平文を暗号化してメモリ部に記憶し、

30 前記登録手段は、パスワードの入力を受け付け、前記鍵情報を用いて前記パスワードを暗号化して暗号化パスワードを生成し、生成した前記暗号化パスワードをメモリ部に書き込み、

前記暗号手段は、前記鍵情報を用いて前記暗号化パスワードを復号してパスワードを生成し、ファイル鍵を用いて平文を暗号化して暗号文を生成し、前記パスワードを用いて前記ファイル鍵を暗号化して第 1 暗号化ファイル鍵を生成し、前記鍵情報を用いて前記ファイル鍵を暗号化して第 2 暗号化ファイル鍵を生成し、前記暗号文と前記第 1 及び第 2 暗号化ファイル鍵とを対応付けてメモリ部に書き込み、

前記切換手段は、前記パスワードの入力を受け付け、前記パスワードを用いて前記第 1 暗号化ファイル鍵を復号してファイル鍵を生成する第 1 鍵獲得手段と、前記鍵記録媒体に記憶されている鍵情報を用いて前記第 2 暗号化ファイル鍵を復号してファイル鍵を生成する第 2 鍵獲得手段とを含み、前記第 1 及び第 2 鍵獲得手段のいずれかによりファイル鍵を獲得し、

50 前記復号手段は、前記ファイル鍵を用いて前記暗号文を

5

復号して復号文を生成することを特徴とする請求項18に記載のファイル管理装置。

【請求項20】 前記登録手段は、さらに利用者を識別する利用者識別子の入力を受け付け、前記利用者識別子と対応付けて前記暗号化パスワードをメモリ部に書き込み、

前記暗号手段は、さらに前記利用者識別子の入力を受け付け、前記利用者識別子に対応付けられた前記暗号化パスワードを復号することを特徴とする請求項19に記載のファイル管理装置。

【請求項21】 前記暗号手段は、前記第1暗号化ファイル鍵を生成するか否かを示す指示を受け付け、生成する旨の指示を受け付けた場合に、前記第1暗号化ファイル鍵を生成し、生成しない旨の指示を受け付けた場合に、前記第1暗号化ファイル鍵の生成と、前記第1暗号化ファイル鍵の書き込みとを抑制することを特徴とする請求項19に記載のファイル管理装置。

【請求項22】 前記登録手段は、さらに認証情報を前記暗号化パスワードと対応付けてメモリ部に書き込み、前記暗号手段は、さらに前記暗号化パスワードを復号する場合に、前記認証情報を用いて前記暗号化パスワードの改竄の有無を検証し、

前記暗号手段は、さらに第1暗号化ファイル鍵、第2暗号化ファイル鍵及び暗号文のそれぞれに、対応する認証情報を対応付けてメモリ部に書き込み、

前記第1及び第2鍵復号手段は、さらに第1暗号化ファイル鍵及び第2暗号化ファイル鍵を復号する場合に、それぞれ対応付けられた前記認証情報を用いて改竄の有無を検証し、

前記復号手段は、さらに暗号文を復号する場合に、対応付けられた前記認証情報を用いて改竄の有無を検証することを特徴とする請求項19に記載のファイル管理装置。

【請求項23】 前記登録手段は、前記暗号化パスワードを、前記メモリ部に代えて、前記記録媒体に書き込み、

前記暗号手段は、前記記録媒体に書き込まれている前記暗号化パスワードを復号することを特徴とする請求項19に記載のファイル管理装置。

【請求項24】 前記登録手段は、さらに新パスワードの入力を受け付け、前記暗号情報を用いて前記新パスワードを暗号化して新暗号化パスワードを生成し、前記暗号化パスワードに代えて、生成した前記新暗号化パスワードをメモリ部に書き込み、

前記暗号手段は、さらに前記暗号情報を用いて前記第2暗号化ファイル鍵を復号してファイル鍵を生成し、前記新パスワードを用いて前記ファイル鍵を暗号化して新第1暗号化ファイル鍵を生成し、前記第1暗号化ファイル鍵に代えて、前記新第1暗号化ファイル鍵をメモリ部に書き込むことを特徴とする請求項19に記載のファイル管

(4) 特開2002-33727

6

理装置。

【請求項25】 前記登録手段は、さらに利用者を識別する利用者識別子の入力を受け付け、

前記暗号手段は、さらに前記利用者識別子を、前記暗号文、前記第1暗号化ファイル鍵及び前記第2暗号化ファイル鍵に対応付けてメモリ部に書き込み、

前記暗号手段は、前記利用者識別子に対応づけられた前記第2暗号化ファイル鍵を検索し、検索した前記第2暗号化ファイル鍵を復号することを特徴とする請求項24に記載のファイル管理装置。

【請求項26】 前記暗号手段は、さらに暗号化を示す暗号化情報と、前記暗号文、前記第1暗号化ファイル鍵及び前記第2暗号化ファイル鍵に対応付けてメモリ部に書き込み、

前記暗号手段は、前記暗号化情報が対応づけられた前記第2暗号化ファイル鍵を検索し、検索した前記第2暗号化ファイル鍵を復号することを特徴とする請求項24に記載のファイル管理装置。

【請求項27】 前記登録手段は、さらに利用者を識別する利用者識別子の入力を受け付け、

前記暗号手段は、さらに前記利用者識別子と、前記暗号文、前記第1暗号化ファイル鍵及び前記第2暗号化ファイル鍵を識別するファイル識別子とを対応付けて一括ファイルとしてメモリ部に書き込み、

前記暗号手段は、前記一括ファイルから前記利用者識別子に対応づけられたファイル識別子を抽出し、抽出されたファイル識別子により識別される前記第2暗号化ファイル鍵を特定し、特定された前記第2暗号化ファイル鍵を復号することを特徴とする請求項24に記載のファイル管理装置。

【請求項28】 前記暗号手段は、さらに暗号化を示す暗号化情報と、前記暗号文、前記第1暗号化ファイル鍵及び前記第2暗号化ファイル鍵を識別するファイル識別子とを対応付けて一括ファイルとしてメモリ部に書き込み、

前記暗号手段は、前記一括ファイルから前記暗号化情報に対応づけられたファイル識別子を抽出し、抽出されたファイル識別子により識別される前記第2暗号化ファイル鍵を特定し、特定された前記第2暗号化ファイル鍵を復号することを特徴とする請求項24に記載のファイル管理装置。

【請求項29】 前記ファイル管理装置は、さらに、メモリ部に書き込まれている前記第2暗号化ファイル鍵を削除する削除手段を含むことを特徴とする請求項19に記載のファイル管理装置。

【請求項30】 前記記録媒体は、前記暗号情報に代えて、新暗号情報を予め記憶しており、

前記登録手段は、前記パスワードの入力を受け付け、前記新暗号情報を用いて前記パスワードを暗号化して新暗号化パスワードを生成し、前記暗号化パスワードに代え

7

て、生成した前記新暗号化パスワードをメモリ部に書き込み、

前記暗号手段は、前記パスワードを用いて前記第1暗号化ファイル鍵を復号してファイル鍵を生成し、前記鍵情報を用いて前記ファイル鍵を暗号化して前記第2暗号化ファイル鍵を生成し、前記第2暗号化ファイル鍵に代えて、前記新第2暗号化ファイル鍵を前記メモリ部に書き込むことを特徴とする請求項19に記載のファイル管理装置。

【請求項31】 前記登録手段は、さらに利用者を識別する利用者識別子の入力を受け付け、前記暗号手段は、さらに前記利用者識別子を、前記暗号文、前記第1暗号化ファイル鍵及び前記第2暗号化ファイル鍵に対応付けてメモリ部に書き込み、

前記暗号手段は、前記利用者識別子に対応づけた前記第1暗号化ファイル鍵を検索し、検索した前記第1暗号化ファイル鍵を復号することと特徴とする請求項30に記載のファイル管理装置。

【請求項32】 前記暗号手段は、さらに暗号化を示す暗号化情報を、前記暗号文、前記第1暗号化ファイル鍵及び前記第2暗号化ファイル鍵に対応付けてメモリ部に書き込み、

前記暗号手段は、前記暗号化情報が対応づけた前記第1暗号化ファイル鍵を検索し、検索した前記第1暗号化ファイル鍵を復号することと特徴とする請求項30に記載のファイル管理装置。

【請求項33】 前記登録手段は、さらに利用者を識別する利用者識別子の入力を受け付け、前記暗号手段は、さらに前記利用者識別子と、前記暗号文、前記第1暗号化ファイル鍵及び前記第2暗号化ファイル鍵を識別するファイル識別子とを対応付けて一括ファイルとしてメモリ部に書き込み、

前記暗号手段は、前記一括ファイルから前記利用者識別子に対応づけたファイル識別子を抽出し、抽出されたファイル識別子により識別される前記第1暗号化ファイル鍵を特定し、特定された前記第1暗号化ファイル鍵を復号することと特徴とする請求項30に記載のファイル管理装置。

【請求項34】 前記暗号手段は、さらに暗号化を示す暗号化情報を、前記暗号文、前記第1暗号化ファイル鍵及び前記第2暗号化ファイル鍵を識別するファイル識別子とを対応付けて一括ファイルとしてメモリ部に書き込み、

前記暗号手段は、前記一括ファイルから前記暗号化情報に対応づけたファイル識別子を抽出し、抽出されたファイル識別子により識別される前記第1暗号化ファイル鍵を特定し、特定された前記第1暗号化ファイル鍵を復号することと特徴とする請求項30に記載のファイル管理装置。

【請求項35】 前記切替手段は、さらに、前記パsw

(5)

特開2002-33727

8

ードの入力を受け付け、前記パスワードを用いて前記第1暗号化ファイル鍵を復号して第1ファイル鍵を生成し、前記鍵情報を用いて前記第2暗号化ファイル鍵を復号して第2ファイル鍵を生成し、前記第1ファイル鍵と前記第2ファイル鍵とが一致するかどうかを判断し、一致しない場合に、エラーとすることを特徴とする請求項19に記載のファイル管理装置。

【請求項36】 平文を暗号化してメモリ部に記憶するファイル暗号装置であって、

鍵情報を予め記憶している鍵記録媒体と、パスワードの入力を受け付け、前記鍵情報を用いて前記パスワードを暗号化して暗号化パスワードを生成し、生成した前記暗号化パスワードをメモリ部に書き込む登録手段と、

前記鍵情報を用いて前記暗号化パスワードを復号してパスワードを生成し、ファイル鍵を用いて平文を暗号化して暗号文を生成し、前記パスワードを用いて前記ファイル鍵を暗号化して第1暗号化ファイル鍵を生成し、前記鍵情報を用いて前記ファイル鍵を暗号化して第2暗号化ファイル鍵を生成し、前記暗号文と前記第1及び第2暗号化ファイル鍵とを対応付けてメモリ部に書き込む暗号手段とを備えることを特徴とするファイル暗号装置。

【請求項37】 請求項35のファイル暗号装置により生成された前記暗号文と前記第1暗号化ファイル鍵と前記第2暗号化ファイル鍵とが対応付けてメモリ部に記憶されており、前記暗号文を復号するファイル復号装置であって、

鍵情報を予め記憶している鍵記録媒体と、前記パスワードの入力を受け付け、前記パスワードを用いて前記第1暗号化ファイル鍵を復号してファイル鍵を生成する第1鍵獲得手段と、前記鍵記録媒体に記憶されている鍵情報を用いて前記第2暗号化ファイル鍵を復号してファイル鍵を生成する第2鍵獲得手段とを含み、前記第1及び第2鍵獲得手段のいずれかによりファイル鍵を獲得する切替手段と、

前記ファイル鍵を用いて前記暗号文を復号して復号文を生成する復号手段とを備えることを特徴とするファイル復号装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、情報を暗号化して記憶し、第三者への情報漏洩を防止するファイル管理装置に関する。

【0002】

【従来の技術】 コンピュータの普及に伴い、情報が第三者へ漏洩しないように、情報を暗号化して記憶する技術が一般に用いられるようになってきている。特開平9-204330号公報により開示されている技術によると、計算機内のファイルがある暗号鍵を用いて暗号化されて特定の暗号情報格納領域に格納され、特定の利用

(6)

特開2002-33727

9

のみが前記暗号情報納領域にアクセスできるように、認証パスワードが登録され、前記利用者は、前記認証パスワードを記憶しておく。前記利用者が、記憶している前記認証パスワードを入力すると、復号鍵が自動的に選ばれて暗号化されたファイルが復号される。ここで、前記認証パスワードは、人が記憶できる程度に短い文字列や数字であり、前記暗号鍵、又は前記復号鍵は、前記認証パスワードと比べて長いビット数のものである。

【0003】

【発明が解決しようとする課題】しかしながら、利用者は、前記認証パスワードを覚えておかなければならず、利用者が前記認証パスワードを忘れてしまった場合には、暗号化された情報が復号できないという問題点がある。上記の問題点を解決するために、本発明は、暗号化された情報を安全に管理でき、さらに利用者がパスワードを忘れた場合であっても、暗号化された情報が確実に復号できるファイル管理装置を提供することを目的とする。

【0004】

【課題を解決するための手段】上記目的を達成するために、本発明は、平文を暗号化して記憶し、復号するファイル管理装置であって、鍵情報を予め記憶している鍵記録媒体と、入力されるパスワードを用いて前記鍵情報を暗号化して暗号化鍵を生成する登録手段と、前記鍵記録媒体に記憶されている鍵情報に基づいて、平文を暗号化して暗号文を生成する暗号手段と、前記鍵記録媒体から鍵情報を読み出すか、又は入力されるパスワードを用いて前記暗号化鍵を復号して鍵情報を生成するかを切り換える切替手段と、前記鍵情報に基づいて暗号文を復号する復号手段とを備えることを特徴とする。

【0005】ここで、前記ファイル管理装置は、さらにメモリ部を有し、前記登録手段は、パスワードの入力を受け付け、前記パスワードを用いて前記鍵情報を暗号化して暗号化鍵を生成し、生成した前記暗号化鍵をメモリ部に書き込み、前記暗号手段は、ファイル鍵を用いて平文を暗号化して暗号文を生成し、前記鍵情報を用いて前記ファイル鍵を暗号化して暗号化ファイル鍵を生成し、前記暗号文と前記暗号化ファイル鍵とを対応付けてメモリ部に書き込み、前記切替手段は、前記パスワードの入力を受け付け、前記パスワードを用いて前記暗号化鍵を復号して鍵情報を生成する第1鍵獲得手段と、第2タイプの入力を受け付けた場合に、前記鍵記録媒体から鍵情報を読み出す第2鍵獲得手段とを含み、前記切替手段は、前記第1及び第2鍵獲得手段のいずれかにより鍵情報を獲得し、前記復号手段は、前記鍵情報を用いて前記暗号化ファイル鍵を復号してファイル鍵を生成し、前記ファイル鍵を用いて前記暗号文を復号して復号文を生成するように構成してもよい。

【0006】ここで、前記登録手段は、さらに利用者を識別する利用者識別子の入力を受け付け、前記利用者識

10

別子と対応付けて前記暗号化鍵をメモリ部に書き込み、前記第1鍵獲得手段は、さらに前記利用者識別子の入力を受け付け、前記利用者識別子に対応付けられた前記暗号化鍵を復号するように構成してもよい。ここで、前記登録手段は、さらに前記鍵情報又は認証情報を前記暗号化鍵と対応付けてメモリ部に書き込み、前記暗号手段は、さらに前記暗号化鍵、前記鍵情報又は認証情報を前記暗号文と対応付けてメモリ部に書き込み、前記第1鍵獲得手段は、さらに前記認証情報が対応付けられた前記暗号化鍵を復号する場合に、前記認証情報を用いて前記暗号化鍵の改竄の有無を検査し、前記復号手段は、さらに前記認証情報が対応付けられた前記暗号文を復号する場合に、前記認証情報を用いて前記暗号文の改竄の有無を検査するように構成してもよい。

【0007】ここで、前記登録手段は、前記暗号化鍵を可搬型記録媒体であるメモリ部に書き込み、前記第1鍵獲得手段は、前記可搬型記録媒体であるメモリ部に書き込まれている前記暗号化鍵を復号するように構成してもよい。ここで、前記ファイル管理装置は、さらに、メモリ部に書き込まれている前記暗号化鍵を削除する削除手段を含むように構成してもよい。

【0008】ここで、前記ファイル管理装置は、さらに、メモリ部に書き込まれている前記暗号化鍵を削除する削除手段を含み、前記登録手段は、さらに、新パスワードの入力を受け付け、前記新パスワードを用いて前記鍵情報を暗号化して新暗号化鍵を生成し、生成した前記新暗号化鍵をメモリ部に書き込むように構成してもよい。

【0009】ここで、前記鍵記録媒体は、前記鍵情報に代えて、新鍵情報を予め記憶しており、前記登録手段は、さらに前記パスワードの入力を受け付け、前記パスワードを用いて前記暗号化鍵を復号して鍵情報を生成し、前記暗号手段は、さらに前記鍵情報を用いて前記暗号化ファイル鍵を復号してファイル鍵を生成し、前記新鍵情報を用いて前記ファイル鍵を暗号化して新暗号化ファイル鍵を生成し、前記暗号化ファイル鍵に代えて前記新暗号化ファイル鍵をメモリ部に書き込み、前記登録手段は、さらに前記パスワードを用いて前記新鍵情報を暗号化して新暗号化鍵を生成し、前記暗号化鍵に代えて生成した前記新暗号化鍵をメモリ部に書き込むように構成してもよい。

【0010】ここで、前記登録手段は、さらに利用者を識別する利用者識別子の入力を受け付け、前記暗号手段は、さらに前記利用者識別子を前記暗号文及び前記暗号化ファイル鍵に対応付けてメモリ部に書き込み、前記暗号手段は、メモリ部内において前記利用者識別子に対応づけられた前記暗号化ファイル鍵を検査し、検索された前記暗号化ファイル鍵からファイル鍵を生成するように構成してもよい。

【0011】ここで、前記暗号手段は、さらに暗号化を

-6-

(7) 特開2002-33727

11

示す暗号化情報を前記暗号文及び前記暗号化ファイル鍵に対応付けてメモリ部に書き込み、前記暗号手段は、メモリ部内において暗号化情報に対応づけられた前記暗号化ファイル鍵を検索し、検索された前記暗号化ファイル鍵からファイル鍵を生成するように構成してもよい。ここで、前記登録手段は、さらに利用者を識別する利用者識別子の入力を受け付け、前記暗号手段は、さらに前記利用者識別子と、前記暗号文及び前記暗号化ファイル鍵を識別するファイル識別子とを対応付けて一括ファイルとしてメモリ部に書き込み、前記暗号手段は、前記一括ファイルから前記利用者識別子に対応づけられたファイル識別子を抽出し、抽出されたファイル識別子により識別される前記暗号化ファイル鍵を特定し、特定された前記暗号化ファイル鍵からファイル鍵を生成するように構成してもよい。

【0012】ここで、前記暗号手段は、さらに暗号化を示す暗号化情報と、前記暗号文及び前記暗号化ファイル鍵を識別するファイル識別子とを対応付けて一括ファイルとしてメモリ部に書き込み、前記暗号手段は、前記一括ファイルから前記暗号化情報に対応づけられたファイル識別子を抽出し、抽出されたファイル識別子により識別される前記暗号化ファイル鍵を特定し、特定された前記暗号化ファイル鍵からファイル鍵を生成するように構成してもよい。

【0013】ここで、前記暗号手段は、さらに前記暗号化鍵を前記暗号文及び前記暗号化ファイル鍵に対応付けてメモリ部に書き込み、前記第1鍵獲得手段は、前記暗号文及び前記暗号化ファイル鍵と対応付けて記憶されている前記暗号化鍵を復号するように構成してもよい。ここで、前記暗号手段は、さらに、暗号化鍵と暗号文とを対応付けてメモリ部に書き込むか否かを示す指示の入力を受け付け、前記指示が対応付けて書き込むことを示す場合に、前記暗号化鍵を前記暗号文と対応付けてメモリ部に書き込むように構成してもよい。

【0014】ここで、前記登録手段は、生成した前記暗号化鍵を、メモリ部に代えて、前記記録媒体に書き込むように構成してもよい。また、本発明は、平文を暗号化してメモリ部に記憶するファイル暗号装置であって、鍵情報を予め記憶している鍵記録媒体と、パスワードの入力を受け付け、前記パスワードを用いて前記鍵情報を暗号化して暗号化鍵を生成し、生成した前記暗号化鍵をメモリ部に書き込む登録手段と、ファイル鍵を用いて平文を暗号化して暗号文を生成し、前記鍵情報を用いて前記ファイル鍵を暗号化して暗号化ファイル鍵を生成し、前記暗号文と前記暗号化ファイル鍵とを対応付けてメモリ部に書き込む暗号手段とを備えることを特徴とする。

【0015】また、本発明は、前記ファイル暗号装置により生成された前記暗号文と前記暗号化ファイル鍵とが対応付けてメモリ部に記憶されており、前記暗号文を復

12

号するファイル復号装置であって、鍵情報を予め記憶している鍵記録媒体と、前記パスワードの入力を受け付け、前記パスワードを用いて前記暗号化鍵を復号して鍵情報を生成する第1鍵獲得手段と、前記鍵記録媒体から鍵情報を読み出す第2鍵獲得手段とを含み、前記第1及び第2鍵獲得手段のいずれかにより鍵情報を獲得する切換手段と、前記鍵情報を用いて前記暗号化ファイル鍵を復号してファイル鍵を生成し、前記ファイル鍵を用いて前記暗号文を復号して復号文を生成する復号手段とを備えることを特徴とする。

【0016】また、本発明は、平文を暗号化して記憶し、復号するファイル管理装置であって、鍵情報を予め記憶している鍵記録媒体と、前記鍵情報を用いて入力されるパスワードを暗号化する登録手段と、ファイル鍵を用いて平文を暗号化して暗号文を生成し、前記鍵情報と前記暗号化されたパスワードを復号して得られたパスワードとに基づいて、ファイル鍵を暗号化してそれぞれ暗号化ファイル鍵を生成する暗号手段と、前記鍵情報に基づいて暗号化ファイル鍵を復号するか、又は入力されたパスワードに基づいて暗号化ファイル鍵を復号するかを切り換えて、ファイル鍵を生成する切換手段と、前記ファイル鍵に基づいて暗号文を復号する復号手段とを備えることを特徴とする。

【0017】ここで、前記ファイル管理装置は、平文を暗号化してメモリ部に記憶し、前記登録手段は、パスワードの入力を受け付け、前記鍵情報を用いて前記パスワードを暗号化して暗号化パスワードを生成し、生成した前記暗号化パスワードをメモリ部に書き込み、前記暗号手段は、前記鍵情報を用いて前記暗号化パスワードを復号してパスワードを生成し、ファイル鍵を用いて平文を暗号化して暗号文を生成し、前記パスワードを用いて前記ファイル鍵を暗号化して第1暗号化ファイル鍵を生成し、前記鍵情報を用いて前記ファイル鍵を暗号化して第2暗号化ファイル鍵を生成し、前記暗号文と前記第1及び第2暗号化ファイル鍵とを対応付けてメモリ部に書き込み、前記切換手段は、前記パスワードの入力を受け付け、前記パスワードを用いて前記第1暗号化ファイル鍵を復号してファイル鍵を生成する第1鍵獲得手段と、前記鍵記録媒体に記憶されている鍵情報を用いて前記第2暗号化ファイル鍵を復号してファイル鍵を生成する第2鍵獲得手段とを含み、前記第1及び第2鍵獲得手段のいずれかによりファイル鍵を獲得し、前記復号手段は、前記ファイル鍵を用いて前記暗号文を復号して復号文を生成するように構成してもよい。

【0018】ここで、前記登録手段は、さらに利用者を識別する利用者識別子の入力を受け付け、前記利用者識別子と対応付けて前記暗号化パスワードをメモリ部に書き込み、前記暗号手段は、さらに前記利用者識別子の入力を受け付け、前記利用者識別子に対応付けられた前記暗号化パスワードを復号するように構成してもよい。こ

(8) 特開2002-33727

13

ここで、前記暗号手段は、前記第1暗号化ファイル鍵を生成するか否かを示す指示を受け付け、生成する旨の指示を受け付けた場合に、前記第1暗号化ファイル鍵を生成し、生成しない旨の指示を受け付けた場合に、前記第1暗号化ファイル鍵の生成と、前記第1暗号化ファイル鍵の書き込みとを抑制するように構成してもよい。

【0019】ここで、前記登録手段は、さらに認証情報を前記暗号化パスワードと対応付けてメモリ部に書き込み、前記暗号手段は、さらに前記暗号化パスワードを復号する場合に、前記認証情報を用いて前記暗号化パスワードの改竄の有無を検証し、前記暗号手段は、さらに第1暗号化ファイル鍵、第2暗号化ファイル鍵及び暗号文のそれぞれに、対応する認証情報を対応付けてメモリ部に書き込み、前記第1及び第2鍵復号手段は、さらに第1暗号化ファイル鍵及び第2暗号化ファイル鍵を復号する場合に、それぞれ対応付けられた前記認証情報を用いて改竄の有無を検証し、前記復号手段は、さらに暗号文を復号する場合に、対応付けられた前記認証情報を用いて改竄の有無を検証するように構成してもよい。

【0020】ここで、前記登録手段は、前記暗号化パスワードを、前記メモリ部に代えて、前記鍵記録媒体に書き込み、前記暗号手段は、前記鍵記録媒体に書き込まれている前記暗号化パスワードを復号するように構成してもよい。ここで、前記登録手段は、さらに新パスワードの入力を受け付け、前記鍵情報を用いて前記新パスワードを暗号化して新暗号化パスワードを生成し、前記暗号化パスワードに代えて、生成した前記新暗号化パスワードをメモリ部に書き込み、前記暗号手段は、さらに前記鍵情報を用いて前記第2暗号化ファイル鍵を復号してファイル鍵を生成し、前記新パスワードを用いて前記ファイル鍵を暗号化して新第1暗号化ファイル鍵を生成し、前記第1暗号化ファイル鍵に代えて、前記新第1暗号化ファイル鍵をメモリ部に書き込むように構成してもよい。

【0021】ここで、前記登録手段は、さらに利用者を識別する利用者識別子の入力を受け付け、前記暗号手段は、さらに前記利用者識別子を、前記暗号文、前記第1暗号化ファイル鍵及び前記第2暗号化ファイル鍵に対応付けてメモリ部に書き込み、前記暗号手段は、前記利用者識別子に対応づけられた前記第2暗号化ファイル鍵を

検索し、検索した前記第2暗号化ファイル鍵を復号するように構成してもよい。

【0022】ここで、前記暗号手段は、さらに暗号化を示す暗号化情報を、前記暗号文、前記第1暗号化ファイル鍵及び前記第2暗号化ファイル鍵に対応付けてメモリ部に書き込み、前記暗号手段は、前記暗号化情報が対応づけられた前記第2暗号化ファイル鍵を検索し、検索した前記第2暗号化ファイル鍵を復号するように構成してもよい。

【0023】ここで、前記登録手段は、さらに利用者を

14

識別する利用者識別子の入力を受け付け、前記暗号手段は、さらに前記利用者識別子と、前記暗号文、前記第1暗号化ファイル鍵及び前記第2暗号化ファイル鍵を識別するファイル識別子とを対応付けて一括ファイルとしてメモリ部に書き込み、前記暗号手段は、前記一括ファイルから前記利用者識別子に対応づけられたファイル識別子を抽出し、抽出されたファイル識別子により識別される前記第2暗号化ファイル鍵を特定し、特定された前記第2暗号化ファイル鍵を復号するように構成してもよい。

【0024】ここで、前記暗号手段は、さらに暗号化を示す暗号化情報と、前記暗号文、前記第1暗号化ファイル鍵及び前記第2暗号化ファイル鍵を識別するファイル識別子とを対応付けて一括ファイルとしてメモリ部に書き込み、前記暗号手段は、前記一括ファイルから前記暗号化情報に対応づけられたファイル識別子を抽出し、抽出されたファイル識別子により識別される前記第2暗号化ファイル鍵を特定し、特定された前記第2暗号化ファイル鍵を復号するように構成してもよい。

【0025】ここで、前記ファイル管理装置は、さらに、メモリ部に書き込まれている前記第2暗号化ファイル鍵を削除する削除手段を含むように構成してもよい。ここで、前記鍵記録媒体は、前記鍵情報に代えて、新鍵情報を予め記憶しており、前記登録手段は、前記パスワードの入力を受け付け、前記新鍵情報を用いて前記パスワードを暗号化して新暗号化パスワードを生成し、前記暗号化パスワードに代えて、生成した前記新暗号化パスワードをメモリ部に書き込み、前記暗号手段は、前記パスワードを用いて前記第1暗号化ファイル鍵を復号してファイル鍵を生成し、前記新鍵情報を用いて前記ファイル鍵を暗号化して新第2暗号化ファイル鍵を生成し、前記第2暗号化ファイル鍵に代えて、前記新第2暗号化ファイル鍵を前記メモリ部に書き込むように構成してもよい。

【0026】ここで、前記登録手段は、さらに利用者を識別する利用者識別子の入力を受け付け、前記暗号手段は、さらに前記利用者識別子を、前記暗号文、前記第1暗号化ファイル鍵及び前記第2暗号化ファイル鍵に対応付けてメモリ部に書き込み、前記暗号手段は、前記利用者識別子に対応づけられた前記第1暗号化ファイル鍵を検索し、検索した前記第1暗号化ファイル鍵を復号するように構成してもよい。

【0027】ここで、前記暗号手段は、さらに暗号化を示す暗号化情報を、前記暗号文、前記第1暗号化ファイル鍵及び前記第2暗号化ファイル鍵に対応付けてメモリ部に書き込み、前記暗号手段は、前記暗号化情報が対応づけられた前記第1暗号化ファイル鍵を検索し、検索した前記第1暗号化ファイル鍵を復号するように構成してもよい。

【0028】ここで、前記登録手段は、さらに利用者を

15

識別する利用者識別子の入力を受け付け、前記暗号手段は、さらに前記利用者識別子と、前記暗号文、前記第1暗号化ファイル鍵及び前記第2暗号化ファイル鍵を識別するファイル識別子とを対応付けて一括ファイルとしてメモリ部に書き込み、前記暗号手段は、前記一括ファイルから前記利用者識別子に対応づけられたファイル識別子を抽出し、抽出されたファイル識別子により識別される前記第1暗号化ファイル鍵を特定し、特定された前記第1暗号化ファイル鍵を復号するように構成してもよい。

【0029】ここで、前記暗号手段は、さらに暗号化を示す暗号化情報と、前記暗号文、前記第1暗号化ファイル鍵及び前記第2暗号化ファイル鍵を識別するファイル識別子とを対応付けて一括ファイルとしてメモリ部に書き込み、前記暗号手段は、前記一括ファイルから前記暗号化情報に対応づけられたファイル識別子を抽出し、抽出されたファイル識別子により識別される前記第1暗号化ファイル鍵を特定し、特定された前記第1暗号化ファイル鍵を復号するように構成してもよい。

【0030】ここで、前記切替手段は、さらに、前記パスワードの入力を受け付け、前記パスワードを用いて前記第1暗号化ファイル鍵を復号して第1ファイル鍵を生成し、前記鍵情報を用いて前記第2暗号化ファイル鍵を復号して第2ファイル鍵を生成し、前記第1ファイル鍵と前記第2ファイル鍵とが一致するか否かを判断し、一致しない場合に、エラーとするように構成してもよい。

【0031】また、本発明は、平文を暗号化してメモリ部に記憶するファイル暗号装置であって、鍵情報を予め記憶している鍵記録媒体と、パスワードの入力を受け付け、前記鍵情報を用いて前記パスワードを暗号化して暗号化パスワードを生成し、生成した前記暗号化パスワードをメモリ部に書き込む登録手段と、前記鍵情報を用いて前記暗号化パスワードを復号してパスワードを生成し、ファイル鍵を用いて平文を暗号化して暗号文を生成し、前記パスワードを用いて前記ファイル鍵を暗号化して第1暗号化ファイル鍵を生成し、前記鍵情報を用いて前記ファイル鍵を暗号化して第2暗号化ファイル鍵を生成し、前記暗号文と前記第1及び第2暗号化ファイル鍵とを対応付けてメモリ部に書き込む暗号手段とを備えることを特徴とする。

【0032】また、本発明は、前記ファイル暗号装置により生成された前記暗号文と前記第1暗号化ファイル鍵と前記第2暗号化ファイル鍵とが対応付けてメモリ部に記憶されており、前記暗号文を復号するファイル復号装置であって、鍵情報を予め記憶している鍵記録媒体と、前記パスワードの入力を受け付け、前記パスワードを用いて前記第1暗号化ファイル鍵を復号してファイル鍵を生成する第1鍵獲得手段と、前記鍵記録媒体に記憶されている鍵情報を用いて前記第2暗号化ファイル鍵を復号してファイル鍵を生成する第2鍵獲得手段とを含み、前

(9) 特開2002-33727

16

記第1及び第2鍵獲得手段のいずれかによりファイル鍵を獲得する切替手段と、前記ファイル鍵を用いて前記暗号文を復号して復号文を生成する復号手段とを備えることを特徴とする。

【0033】

【発明の実施の形態】1. 第1の実施の形態

本発明の第1の実施の形態としてのファイル管理装置10について説明する。ファイル管理装置10は、図1に外観を示すように、コンピュータシステムであり、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニット、キーボードなどから構成される。前記RAM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、前記装置は、その機能を実現する。ファイル管理装置10には、鍵情報を予め記録している鍵記録媒体20が装填される。

【0034】1. 1 ファイル管理装置10及び鍵記録媒体20の構成

20 ファイル管理装置10及び鍵記録媒体20の構成について説明する。ファイル管理装置10は、図2に示すように、パスワード登録部100、ファイル暗号部200、ファイル復号部300及び記憶部400から構成されており、鍵記録媒体20が接続される。

【0035】パスワード登録部100は、パスワード入力部101及び暗号化部102から構成され、ファイル暗号部200は、ファイル鍵生成部201、暗号化部202及び暗号化部203から構成され、ファイル復号部300は、パスワード入力部301、復号部302、切替部303、復号部304及び復号部305から構成される。

【0036】(1) 鍵記録媒体20

鍵記録媒体20は、不揮発性の半導体メモリにより構成される記憶領域を備える可搬性のある記録媒体であり、前記記憶領域は、56ビット長の鍵情報を予め記憶している。鍵情報は、1人の利用者に固有の情報である。通常、前記利用者が鍵記録媒体20を所持している。ファイル管理装置10を使用するときに、前記利用者は、鍵記録媒体20をファイル管理装置10の専用の挿入口から装填し、鍵記録媒体20をファイル管理装置10と接続する。

【0037】(2) 記憶部400

記憶部400は、具体的には、ハードディスクユニットから構成され、内部に情報をファイルとして記憶する領域を備えている。各ファイルは、ファイル名により識別される。記憶部400は、あらかじめ、平文を含む平文ファイル401を記憶している。

【0038】(3) パスワード入力部101

パスワード入力部101は、利用者からパスワードの入力を受け付ける。ここで、パスワードは、8文字の数字

17

及び英字からなる文字列である。パスワード入力部101は、受け付けた前記パスワードを暗号化部102へ出力する。

(4) 暗号化部102

暗号化部102は、パスワード入力部101から前記パスワードを受け取る。前記パスワードを受け取ると、暗号化部102は、鍵記録媒体20の記憶領域から鍵情報を読み出し、前記パスワードが56ビット長となるように文字列の最後に複数個の0ビットを付加し、また前記鍵情報が64ビット長となるように前記鍵情報の最後に複数個の0ビットを付加する。次に、前記パスワードを鍵として用いて、前記鍵情報に暗号アルゴリズムE1を施して、暗号化鍵を生成する。ここで、暗号アルゴリズムE1は、Data Encryption Standard (以下、DES) によるものである。なお、DESについては、公知であるので説明を省略する。

【0039】なお、図2に示すブロック図において、パスワード入力部101を示すブロックと暗号化部102を示すブロックとを結ぶ線の付近に鍵を示すマークを表示している。このマークは、暗号化部102において、パスワード入力部101から出力されるパスワードを鍵として用いていることを示している。このことは、他の暗号化部、他の復号部についても同様である。また、後述する図10に示すブロック図においても同様である。

【0040】次に、暗号化部102は、生成した前記暗号化鍵を1個のファイルとして記憶部400内に書き込む。

(5) ファイル鍵生成部201

ファイル鍵生成部201は、内部に乱数発生部とタイマとを備え、56ビット長の乱数を生成し、年、月、日、時、分、秒及びミリ秒からなる現在時刻を取得し、生成した前記乱数と取得した現在時刻とに排他的論理和を施して56ビット長のファイル鍵を生成し、生成したファイル鍵を暗号化部202及び暗号化部203へ出力する。

【0041】(6) 暗号化部203

暗号化部203は、利用者から記憶部400に記憶されている平文ファイル401のファイル名の指定を受け付け、指定を受け付けたファイル名により特定される平文ファイル401を記憶部400から読み出す。また、ファイル鍵生成部201からファイル鍵を受け取る。

【0042】次に、暗号化部203は、受け取ったファイル鍵を鍵として用いて、平文ファイル401内に含まれる平文に暗号アルゴリズムE3を施して暗号文を生成する。次に、ヘッダ部とデータ部とを含むファイルであって、データ部内に生成した前記暗号文を含む暗号化ファイル404を記憶部400に書き込む。ここで、暗号アルゴリズムE3は、DESによるものである。

【0043】ここで、前記平文が64ビット長以上の場

(10)

特開2002-33727

18

合には、暗号化部203は、前記平文を複数個の64ビット長の平文ブロックに分割し、各平文ブロック毎に暗号アルゴリズムE3を施して暗号化ブロックを生成し、生成した複数の暗号化ブロックを結合して、暗号文とする。

(7) 暗号化部202

暗号化部202は、鍵記録媒体20から鍵情報を読み出し、ファイル鍵生成部201からファイル鍵を受け取り、前記ファイル鍵が64ビット長となるように前記ファイル鍵の最後に複数個の0ビットを付加する。

【0044】次に、暗号化部202は、読み出した鍵情報を鍵として用いて、前記ファイル鍵に暗号アルゴリズムE2を施して暗号化ファイル鍵を生成し、生成した前記暗号化ファイル鍵を、記憶部400の暗号化ファイル404内のヘッダ部に書き込む。ここで、暗号アルゴリズムE2は、DESによるものである。

(8) 切換部303

切換部303は、利用者から第1及び第2タイプのいずれかの入力を受け付ける。第1タイプは、パスワードを用いて暗号文を復号することを示し、第2タイプは、鍵情報を用いて暗号文を復号することを示す。

【0045】切換部303は、第1タイプの入力を受け付けた場合には、復号部302から鍵情報を受け取り、受け取った前記鍵情報を復号部304へ出力する。第2タイプの入力を受け付けた場合には、鍵記録媒体20から鍵情報を読み出し、読み出した前記鍵情報を復号部304へ出力する。

(9) パスワード入力部301

パスワード入力部301は、パスワード入力部101と同様に、利用者からパスワードの入力を受け付け、受け付けた前記パスワードを復号部302へ出力する。

【0046】(10) 復号部302

復号部302は、パスワード入力部301からパスワードを受け取り、記憶部400から暗号化鍵を読み出し、前記パスワードの長さが56ビット長となるように、前記パスワードの最後に複数個の0ビットを付加し、前記パスワードを鍵として用いて、読み出した前記暗号化鍵に復号アルゴリズムD1を施して鍵情報を生成する。ここで、復号アルゴリズムD1は、DESによるものであり、暗号アルゴリズムE1の逆変換を行うアルゴリズムである。

【0047】次に、復号部302は、鍵情報の先頭56ビット長を残して、前記鍵情報から残りのビット列を削除し、56ビット長の前記鍵情報を切換部303へ出力する。

(11) 復号部304

復号部304は、切換部303から鍵情報を受け取り、記憶部400から暗号化ファイル404のヘッダ部に含まれる暗号化ファイル鍵を読み出し、受け取った前記鍵情報を鍵として用いて、読み出した暗号化ファイル鍵に

(11)

特開2002-33727

19

復号アルゴリズムD2を施してファイル鍵を生成する。
ここで、復号アルゴリズムD2は、DESによるものであり、暗号アルゴリズムE2の逆変換を行うアルゴリズムである。

【0048】次に、復号部304は、生成したファイル鍵の先頭56ビット長を残して、前記ファイル鍵から残りのビット列を削除し、56ビット長の前記ファイル鍵を復号部305へ出力する。

(12) 復号部305

復号部305は、復号部304からファイル鍵を受け取り、記憶部400から暗号化ファイル404のデータ部に含まれる暗号文を読み出し、受け取った前記ファイル鍵を鍵として用いて、読み出した暗号文に復号アルゴリズムD3を施して復号文を生成する。ここで、復号アルゴリズムD3は、DESによるものであり、暗号アルゴリズムE3の逆変換を行うアルゴリズムである。

【0049】ここで、前記暗号文が64ビット長以上の場合には、復号部305は、前記暗号文を複数個の64ビット長の暗号文ブロックに分割し、各暗号文ブロック毎に復号アルゴリズムD3を施して復号文ブロックを生成し、生成した複数の復号文ブロックを結合して、復号文とする。次に、復号部305は、生成した前記復号文を含む復号文ファイル402を記憶部400内に書き込む。

【0050】1. 2 ファイル管理装置10の動作
ファイル管理装置10の動作について説明する。

(1) パスワード登録部100の動作

パスワード登録部100の動作について、図3に示すフローチャートを用いて説明する。

【0051】パスワード入力部101は、利用者からパスワードの入力を受け付け、受け付けた前記パスワードを暗号化部102へ出力する(ステップS101)。次に、暗号化部102は、記録媒体20の記憶領域から鍵情報を読み出し(ステップS102)、前記パスワードを鍵として用いて、前記鍵情報に暗号アルゴリズムE1を施して、暗号化鍵を生成し(ステップS103)、生成した前記暗号化鍵を1個のファイルとして記憶部400内に書き込む(ステップS104)。

【0052】(2) ファイル暗号部200の動作

ファイル暗号部200の動作について、図4に示すフローチャートを用いて説明する。ファイル鍵生成部201は、ファイル鍵を生成する(ステップS121)。次に、暗号化部203は、平文ファイル401を記憶部400から読み出し、ファイル鍵を鍵として用いて、平文ファイル401内に含まれる平文に暗号アルゴリズムE3を施して暗号文を生成し(ステップS122)、データ部内に生成した前記暗号文を含む暗号化ファイル404を記憶部400に書き込む(ステップS123)。

【0053】次に、暗号化部202は、記録媒体20から鍵情報を読み出し、ファイル鍵生成部201からフ

20

ァイル鍵を受け取り、読み出した鍵情報を鍵として用いて、前記ファイル鍵に暗号アルゴリズムE2を施して暗号化ファイル鍵を生成し、(ステップS124)、生成した前記暗号化ファイル鍵を、記憶部400の暗号化ファイル404内のヘッダ部内に書き込む(ステップS125)。

【0054】(3) ファイル復号部300の動作

ファイル復号部300の動作について、図5に示すフローチャートを用いて説明する。切換部303は、利用者から第1及び第2タイプのいずれかの入力を受け付ける(ステップS141)。

【0055】切換部303が第1タイプの入力を受け付けた場合には、(ステップS142)、パスワード入力部301は、利用者からパスワードの入力を受け付け、受け付けた前記パスワードを復号部302へ出力し(ステップS144)、復号部302は、記憶部400から暗号化鍵を読み出し、前記パスワードを鍵として用いて、読み出した前記暗号化鍵に復号アルゴリズムD1を施して鍵情報を生成し、前記鍵情報を切換部303を介して復号部304へ出力する(ステップS145)。

【0056】切換部303が第2タイプの入力を受け付けた場合には(ステップS142)、切換部303は、記録媒体20から鍵情報を読み出し、読み出した前記鍵情報を復号部304へ出力する(ステップS143)。

次に、復号部304は、切換部303から鍵情報を受け取り、記憶部400から暗号化ファイル404のヘッダ部に含まれる暗号化ファイル鍵を読み出し、受け取った前記鍵情報を鍵として用いて、読み出した暗号化ファイル鍵に復号アルゴリズムD2を施してファイル鍵を生成し(ステップS146)、復号部305は、記憶部400から暗号化ファイル404のデータ部に含まれる暗号文を読み出し、前記ファイル鍵を鍵として用いて、読み出した暗号文に復号アルゴリズムD3を施して復号文を生成し(ステップS147)、次に、復号部305は、生成した前記復号文を含む復号文ファイル402を記憶部400内に書き込む(ステップS148)。

【0057】1. 3 まとめ

以上説明したように、ファイル管理装置10は、パスワードの登録、平文の暗号化及び暗号文の復号の3つの部分を含んでいる。パスワードの登録時には、利用者は、記録媒体を装填し、登録するパスワードを入力する。パスワード登録部100は、入力されたパスワードを用いて鍵情報を暗号化し、生成された暗号化鍵を計算機内にファイルとして保存する。

【0058】次に、ファイルの暗号時には、利用者は、記録媒体を装填し、暗号化するファイルを指定する。このとき、ファイル毎のパスワード入力が必要であるので、利用者にとって暗号化処理の操作が容易である。ファイル暗号部200は、任意にファイル鍵を生成し、鍵

-11-

21

を生成し、次にファイル鍵を用いてファイルの情報を暗号化して暗号文を生成し、そして暗号化ファイル鍵をヘッダ部に、暗号文をデータ部に含む暗号化ファイルを保存する。

【0059】暗号文の復号には、鍵情報を用いる方法とパスワードを用いる方法とである。鍵情報を用いる場合には、ファイル復号部300は、暗号化ファイルのヘッダ部から獲得した暗号化ファイル鍵を鍵情報を用いて復号してファイル鍵を求め、次に、暗号文をそのファイル鍵で復号する。また、パスワードを用いる場合には、パスワードの入力を受け付け、暗号化鍵をパスワードで復号して鍵情報を求め、さらに鍵情報で暗号化ファイル鍵を復号してファイル鍵を求め、最後にファイル鍵で暗号文を復号してものの平文を求める。

【0060】このように構成されているので、通常は、上記のように鍵情報を用いる方法を利用し、利用者が鍵情報が記録されている鍵記録媒体を持参し忘れた場合には、パスワードを用いる方法により、暗号化された情報を復号することができる。

1. 4 変形例

ファイル管理装置10は、次に示すように構成してもよい。

【0061】(1)パスワード登録部は、さらに利用者識別する利用者識別子(利用者ID)の入力を受け付け、前記利用者IDと対応付けて前記暗号化鍵をメモリ部の利用者IDに書き込むようにしてもよい。図6に利用者IDテーブルの一例を示す。利用者IDテーブルは、利用者IDと暗号化鍵とからなる組を複数個記憶する領域を備えている。このとき、ファイル復号部は、さらに前記利用者IDの入力を受け付け、前記利用者IDテーブルにおいて、入力された前記利用者IDに対応付けられた前記暗号化鍵を復号する。

【0062】このように構成されているので、複数の利用者によりファイル管理装置を利用することができる。

(2)パスワードを変更する場合の動作について、図7に示すフローチャートを用いて説明する。前記ファイル管理装置は、さらに、削除部を含み、前記削除部は、記憶部に書き込まれている前記暗号化鍵を削除する(ステップS161)。

【0063】次に、パスワード登録部100のパスワード入力部101は、利用者から新たなパスワードの入力を受け付け、受け付けた前記パスワードを暗号化部102へ出力する(ステップS162)。次に、暗号化部102は、鍵記録媒体20の記憶領域から鍵情報を読み出し(ステップS163)、前記新たなパスワードを鍵として用いて、前記鍵情報に暗号アルゴリズムE1を施して、新たな暗号化鍵を生成し(ステップS164)、生成した前記新たな暗号化鍵を1個のファイルとして記憶部400内に書き込む(ステップS165)。

【0064】このように、パスワードを更新する場合に

(12)

特開2002-33727

22

は、暗号化鍵を新たに生成すればよい。

(3)パスワードによる復号を禁止するためには、暗号化鍵を削除するだけでよい。

(4)鍵情報を更新する場合のファイル管理装置の動作について、図8に示すフローチャートを用いて説明する。

【0065】前記鍵記録媒体は、前記鍵情報(旧鍵情報と呼ぶ)に代えて、新たな鍵情報(新鍵情報と呼ぶ)を予め記憶している。パスワード入力部101は、前に入力を受け付けたものと同じパスワードの入力を受け付け(ステップS181)、暗号化部102は、前記パスワードを用いて、前記暗号化鍵(旧暗号化鍵と呼ぶ)に復号アルゴリズムD1を施して旧鍵情報を生成し(ステップS182)、鍵記録媒体から新鍵情報を読み出し、前記パスワードを用いて新鍵情報に暗号アルゴリズムE1を施して新暗号化鍵を生成し(ステップS183)、新暗号化鍵を記憶部400に記憶されている旧暗号化鍵に上書きする(ステップS184)。

【0066】次に、ファイル暗号部200は、暗号化ファイル鍵(旧暗号化ファイル鍵と呼ぶ)を読み出して、旧鍵情報を用いて旧暗号化ファイル鍵に復号アルゴリズムD2を施してファイル鍵を生成し(ステップS185)、次に、鍵記録媒体から新鍵情報を読み出し、新鍵情報を用いてファイル鍵に暗号アルゴリズムE2を施して新暗号化ファイル鍵を生成し(ステップS186)、次に、新暗号化ファイル鍵を暗号化ファイル内の旧暗号化ファイル鍵に上書きする(ステップS187)。

【0067】このように、鍵情報を更新する場合に、暗号化鍵とパスワードとを用いて更新前の鍵情報を一旦求めて、鍵情報を用いてヘッダにある暗号化ファイル鍵を復号してファイル鍵を求める。その後新しい鍵情報でファイル鍵を暗号化して、暗号化ファイル鍵を更新する。このとき、暗号化鍵も更新する。この実施の形態においては、鍵情報を紛失した場合に、鍵情報を一時的に無効化することはできない。

【0068】(5)ファイル暗号部は、ファイルを暗号化するときに、暗号化ファイルのヘッダ部に、暗号化がされたか否かを示す暗号化情報を付加するようにしてもよい。このとき、鍵情報を更新する場合において、前記ファイル暗号部は、記憶部内において暗号化情報がヘッダ部に付加された暗号化ファイルから暗号化ファイル鍵を検索し、検索された前記暗号化ファイル鍵からファイル鍵を生成するようにしてもよい。

【0069】また、パスワード登録部は、利用者を識別する利用者IDの入力を受け付け、ファイル暗号部は、さらに前記利用者IDを、前記暗号文及び前記暗号化ファイル鍵を含む暗号化ファイル内に付加して書き込むようにしてもよい。このとき、鍵情報を更新する場合において、ファイル暗号部は、記憶部内において前記利用者IDが付加された暗号化ファイル内の暗号化ファイル鍵

(13) 特開2002-33727

23

を検索し、検索された前記暗号化ファイル鍵からファイル鍵を生成するようにしてもよい。

【0070】また、ファイル暗号化部は、前記利用者IDと、前記暗号文及び前記暗号化ファイル鍵を含む暗号化ファイルを識別するファイル識別子とを対応付けて一括ファイルとして記憶部に書き込むようにしてもよい。このとき、ファイル暗号化部は、前記一括ファイルから前記利用者IDに対応づけられたファイル識別子を抽出し、抽出されたファイル識別子により識別されるファイルに含まれる暗号化ファイル鍵を特定し、特定された前記暗号化ファイル鍵からファイル鍵を生成するようにしてもよい。

【0071】また、ファイル暗号化部は、暗号化を示す暗号化情報と、前記暗号文及び前記暗号化ファイル鍵を含むファイルを識別するファイル識別子とを対応付けて一括ファイルとして記憶部に書き込むようにしてもよい。このとき、ファイル暗号化部は、前記一括ファイルから前記暗号化情報に対応づけられたファイル識別子を抽出し、抽出されたファイル識別子により識別されるファイルに含まれる暗号化ファイル鍵を特定し、特定された前記暗号化ファイル鍵からファイル鍵を生成するようにしてもよい。

【0072】（6）上記の実施の形態では、暗号化鍵は、当該ファイルを暗号化したコンピュータシステム内に保存されているので、パスワードによる暗号文の復号は、当該コンピュータシステム内でのみ可能となる。ここで、他のコンピュータシステムにおいて、パスワードによる復号を可能にするためには、暗号化鍵を可搬型の別記録媒体に格納し、他のコンピュータシステムに入力すればよい。

【0073】ここで、1個のコンピュータシステムのパスワード登録部は、SDメモリーカードなどの可搬型の記録媒体に暗号化鍵を書き込む。また、利用者は、暗号化ファイルを可搬型の記録媒体に書き込む。次に、利用者は、暗号化鍵の書き込まれた記録媒体を他のコンピュータシステムに装填し、他のコンピュータシステムが備えるファイル復号部は、可搬型記録媒体から暗号化鍵を読み出し、復号し、また可搬型記録媒体から暗号文を読み出し、復号する。

【0074】ここで、暗号化鍵と暗号文とを別のファイルにして、1個の可搬型の記録媒体に書き込むようにしてもよい。

（7）パスワード登録部は、鍵記録媒体20から鍵情報を読み出し、読み出した鍵情報にハッシュアルゴリズムを施して第1認証情報を生成し、生成した第1認証情報を前記暗号鍵と対応付けて、記憶部400に書き込むようにしてもよい。このとき、ファイル復号部は、暗号化鍵と第1認証情報とを記憶部から読み出し、暗号化鍵を復号して鍵情報を生成し、生成した前記鍵情報に、上記と

24

同じハッシュアルゴリズムを施して、第2認証情報を生成する。次に、ファイル復号部は、第1認証情報と第2認証情報とを比較して同一でなければ、暗号化鍵が改竄されたものと判断し、同一であれば、暗号化鍵が改竄されていないものと判断する。

【0075】ファイル暗号部は、同様にして、ファイル鍵から認証情報を生成し、生成した認証情報と暗号化ファイル鍵とを対応付けて、記憶部に書き込む。ファイル復号部は、ファイル鍵と認証情報とを読み出し、ファイル鍵から認証情報を生成し、読み出した認証情報と、生成した認証情報とを比較して、ファイル鍵の改竄を検証する。また、平文についても同様である。

【0076】（8）パスワード登録部は、鍵情報を暗号化鍵と対応付けて、記憶部内の同じファイル内に書き込むようにしてもよい。また、ファイル暗号部は、図9に一例として示すように、記憶部内の同じ暗号化ファイルのヘッダ部に暗号化鍵と暗号化ファイル鍵とを書き込み、データ部に暗号文を書き込むようにしてもよい。このとき、ファイル復号部は、記憶部の暗号化鍵を読み出す代わりに、暗号化ファイルのヘッダ部から暗号化鍵を読み出すようにしてもよい。

【0077】暗号化鍵をファイルのヘッダ部に格納することにより、ヘッダ部付きの暗号化ファイルをそのまま他の計算機に移動して、パスワードだけで復号ができる。ただし、パスワードを変更した場合には、対応するファイルのヘッダ部内の暗号化鍵をすべて更新する必要がある。また、ファイル暗号時に、必要となる暗号化鍵と鍵情報を同一の媒体に格納しておくことで便利である。

【0078】（9）ファイル暗号部は、さらに、暗号化鍵と暗号文とを対応付けて1個の暗号化ファイル内に書き込むか否かを示す指示の入力を利用者から受け付け、前記指示が対応付けて書き込むことを示す場合に、前記暗号化鍵をヘッダ部に書き込み、前記暗号文をデータ部に書き込むようにしてもよい。なお、暗号化鍵を格納しないファイルは、暗号化鍵を別途保持していない環境において、パスワードを用いたファイル復号はできない。

【0079】（10）パスワード登録部は、生成した前記暗号化鍵を、記憶部に代えて、前記鍵記録媒体に書き込むようにしてもよい。

2. 第2の実施の形態

本発明の第2の実施の形態としてのファイル管理装置10bについて説明する。

【0080】ファイル管理装置10bは、ファイル管理装置10と同様に、コンピュータシステムであり、鍵記録媒体20が装填される。

2. 1 ファイル管理装置10b及び鍵記録媒体20の構成

ファイル管理装置10b及び鍵記録媒体20の構成について説明する。ファイル管理装置10bは、図10に示すように、パスワード登録部100b、ファイル暗号部

25

200b、ファイル復号部300b及び記憶部400bから構成されており、鍵記録媒体20が接続される。

【0081】パスワード登録部100bは、パスワード入力部101b及び暗号化部102bから構成され、ファイル暗号部200bは、ファイル鍵生成部201b、暗号化部202b、暗号化部203b、暗号化部204b及び復号部205bから構成され、ファイル復号部300bは、パスワード入力部301b、復号部302b、切換部303b、復号部304b及び復号部305bから構成される。

【0082】以下において、ファイル管理装置10の構成部との相違点を中心として説明する。

(1) 記憶部400b

記憶部400bは、記憶部400と同様であり、あらかじめ、平文を含む平文ファイル401bを記憶している。

【0083】(2) パスワード入力部101b

パスワード入力部101bは、パスワード入力部101と同様に、入力を受け付けたパスワードを暗号化部102bへ出力する。

(3) 暗号化部102b

暗号化部102bは、暗号化部102と同様であり、鍵記録媒体20から読み出した鍵情報を鍵として用いて、パスワード入力部101bから受け取ったパスワードに暗号アルゴリズムE1を施して、暗号化パスワードを生成し、生成した暗号化パスワードを1個のファイルとして記憶部400b内に書き込む。

【0084】(4) ファイル鍵生成部201b

ファイル鍵生成部201bは、ファイル鍵生成部201と同様に、ファイル鍵を生成し、生成したファイル鍵を暗号化部202b、暗号化部203b及び暗号化部204bへ出力する。

(5) 復号部205b

復号部205bは、記憶部400bに記憶されている暗号化パスワードを読み出し、鍵記録媒体20から鍵情報を読み出す。次に、読み出した前記鍵情報を用いて、読み出した前記暗号化パスワードに復号アルゴリズムD1を施してパスワードを生成し、生成したパスワードを暗号化部202bへ出力する。

【0085】(6) 暗号化部203b

暗号化部203bは、暗号化部203と同様であり、記憶部400bから平文ファイル401bを読み出し、ファイル鍵生成部201bからファイル鍵を受け取る。次に、暗号化部203bは、受け取ったファイル鍵を鍵として用いて、平文ファイル401bに含まれる平文に暗号アルゴリズムE3を施して暗号文を生成し、データ部内に生成した前記暗号文を含む暗号化ファイル404bを記憶部400bに書き込む。

【0086】(7) 暗号化部202b

暗号化部202bは、復号部205bからパスワードを

(14)

特開2002-33727

26

受け取り、ファイル鍵生成部201bからファイル鍵を受け取る。次に、受け取ったパスワードを鍵として用いて、受け取ったファイル鍵に暗号アルゴリズムE2を施して第1暗号化ファイル鍵を生成し、生成した前記第1暗号化ファイル鍵を、記憶部400bの暗号化ファイル404b内のヘッダ部に書き込む。

【0087】(8) 暗号化部204b

暗号化部204bは、鍵記録媒体20から鍵情報を読み出し、ファイル鍵生成部201bからファイル鍵を受け取る。次に、暗号化部204bは、読み出した鍵情報を鍵として用いて、前記ファイル鍵に暗号アルゴリズムE4を施して第2暗号化ファイル鍵を生成し、生成した前記第2暗号化ファイル鍵を、記憶部400bの暗号化ファイル404b内のヘッダ部に書き込む。ここで、暗号アルゴリズムE4は、DESによるものである。

【0088】(9) 切換部303b

切換部303bは、利用者から第1及び第2タイプのいずれかの入力を受け付ける。第1タイプは、パスワードを用いて暗号文を復号することを示し、第2タイプは、鍵情報を用いて暗号文を復号することを示す。切換部303bは、第1タイプの入力を受け付けた場合には、復号部302bからファイル鍵を受け取り、受け取った前記ファイル鍵を復号部305bへ出力する。第2タイプの入力を受け付けた場合には、復号部304bからファイル鍵を受け取り、受け取った前記ファイル鍵を復号部305bへ出力する。

【0089】(10) パスワード入力部301b

パスワード入力部301bは、パスワード入力部101と同様に、利用者からパスワードの入力を受け付け、受け付けた前記パスワードを復号部302bへ出力する。

(11) 復号部302b

復号部302bは、パスワード入力部301bからパスワードを受け取り、記憶部400bの暗号化ファイル404bのヘッダ部に含まれる第1暗号化ファイル鍵を読み出す。読み出したパスワードを鍵として用いて、読み出した前記第1暗号化ファイル鍵に復号アルゴリズムD2を施してファイル鍵情報を生成し、生成したファイル鍵を切換部303bへ出力する。

【0090】(11) 復号部304b

復号部304bは、鍵記録媒体20から鍵情報を読み出し、記憶部400bの暗号化ファイル404のヘッダ部に含まれる第2暗号化ファイル鍵を読み出し、読み出した前記鍵情報を鍵として用いて、読み出した第2暗号化ファイル鍵に復号アルゴリズムD4を施してファイル鍵を生成する。ここで、復号アルゴリズムD4は、DESによるものであり、暗号アルゴリズムE4の逆変換を行うアルゴリズムである。

【0091】次に、復号部304bは、生成したファイル鍵を切換部303bへ出力する。

(12) 復号部305b

-14-

(15) 特開2002-33727

27

復号部305bは、復号部304bからファイル鍵を受け取り、記憶部400bから暗号化ファイル404bのデータ部に含まれる暗号文を読み出し、受け取った前記ファイル鍵を鍵として用いて、読み出した暗号文に復号アルゴリズムD3を施して復号文を生成する。次に、復号部305bは、生成した前記復号文を含む復号文ファイル402bを記憶部400b内に書き込む。

【0092】2.2 ファイル管理装置10bの動作
ファイル管理装置10bの動作について説明する。

(1) パスワード登録部100bの動作
パスワード登録部100bの動作について、図11に示すフローチャートを用いて説明する。

【0093】パスワード入力部101bは、利用者からパスワードの入力を受け付け、受け付けた前記パスワードを暗号化部102bへ出力する(ステップS201)。次に、暗号化部102bは、鍵記録媒体20の記憶領域から鍵情報を読み出し(ステップS202)、前記鍵情報を鍵として用いて、前記パスワードに暗号アルゴリズムE1を施して、暗号化パスワードを生成し(ステップS203)、生成した前記暗号化パスワードを1つのファイルとして記憶部400b内に書き込む(ステップS204)。

【0094】(2) ファイル暗号部200bの動作
ファイル暗号部200bの動作について、図12に示すフローチャートを用いて説明する。復号部205bは、記憶部400bに記憶されている暗号化パスワードを読み出し、鍵記録媒体20から鍵情報を読み出し、読み出した前記鍵情報を用いて、読み出した前記暗号化パスワードに復号アルゴリズムD1を施してパスワードを生成し、生成したパスワードを暗号化部202bへ出力する(ステップS221)。

【0095】次に、ファイル鍵生成部201bは、ファイル鍵を生成する(ステップS222)。次に、暗号化部203bは、平文ファイル401bを記憶部400bから読み出し、ファイル鍵を鍵として用いて、平文ファイル401b内に含まれる平文に暗号アルゴリズムE3を施して暗号文を生成し(ステップS223)、データ部に生成した前記暗号文を含む暗号化ファイル404bを記憶部400b内に書き込む(ステップS224)。

【0096】次に、暗号化部202bは、パスワードとファイルとを受け取り、パスワードを鍵として用いて、前記ファイル鍵に暗号アルゴリズムE2を施して第1暗号化ファイル鍵を生成し、(ステップS225)、生成した前記第1暗号化ファイル鍵を、記憶部400bの暗号化ファイル404b内のヘッダ部に書き込む(ステップS226)。

【0097】次に、暗号化部204bは、ファイル鍵と鍵情報とを受け取り、鍵情報を鍵として用いて、前記ファイル鍵に暗号アルゴリズムE4を施して第2暗号化ファイル鍵を生成し、(ステップS227)、生成した前

28

記第2暗号化ファイル鍵を、記憶部400bの暗号化ファイル404b内のヘッダ部に書き込む(ステップS228)。

【0098】(3) ファイル復号部300bの動作
ファイル復号部300bの動作について、図13に示すフローチャートを用いて説明する。切換部303bは、利用者から第1及び第2タイプのいずれかの入力を受け付ける(ステップS241)。

【0099】切換部303bが第1タイプの入力を受け付けた場合には、(ステップS242)、パスワード入力部301bは、利用者からパスワードの入力を受け付け、受け付けた前記パスワードを復号部302bへ出力し(ステップS245)、復号部302bは、記憶部400bから第1暗号化ファイル鍵を読み出し、前記パスワードを鍵として用いて、読み出した前記第1暗号化ファイル鍵に復号アルゴリズムD2を施してファイル鍵を生成し、前記ファイル鍵を切換部303bを介して復号部305bへ出力する(ステップS246)。

【0100】切換部303bが第2タイプの入力を受け付けた場合には(ステップS242)、復号部304bは、鍵記録媒体20から鍵情報を読み出し(ステップS243)、記憶部400bから第2暗号化ファイル鍵を読み出し、前記鍵情報を鍵として用いて、読み出した前記第2暗号化ファイル鍵に復号アルゴリズムD4を施してファイル鍵を生成し、前記ファイル鍵を切換部303bを介して復号部305bへ出力する(ステップS244)。

【0101】次に、復号部305bは、記憶部400bから暗号化ファイル404bのデータ部に含まれる暗号文を読み出し、前記ファイル鍵を鍵として用いて、読み出した暗号文に復号アルゴリズムD3を施して復号文を生成し(ステップS247)、次に、復号部305bは、生成した前記復号文を含む復号文ファイル402bを記憶部400b内に書き込む(ステップS248)。

【0102】2.3 まとめ

ファイル管理装置10bは、パスワードの登録、平文の暗号化及び暗号文の復号の3つの部分を含んでいる。パスワードの登録時には、利用者は、鍵情報の記録されている鍵記録媒体を装填し、登録するパスワードを入力する。パスワード登録部100bは、鍵情報を用いて入力されたパスワードを暗号化し、生成された暗号化パスワードをコンピュータシステム内に保存する。第1の実施の形態と比較すると、暗号化の対象となる情報と、暗号化の際に用いられる鍵とが、逆になっている。

【0103】次に、ファイルの暗号時には、利用者は前記暗号化パスワードの存在するコンピュータシステム内において、鍵記録媒体を装填し、暗号化するファイルを指定する。ファイル暗号部200bは、まず前記暗号化パスワードを鍵情報で装填して、パスワードを求める。次に、任意に生成したファイル鍵をこのパスワードを用

(16)

特開2002-33727

29

いて暗号化して第1暗号化ファイル鍵を生成する。また、鍵情報を用いてファイル鍵を暗号化して第2暗号化ファイル鍵を生成する。さらにファイル鍵でファイルの情報を暗号化して暗号文を生成し、そして第1及び第2暗号化ファイル鍵をヘッダ部に、暗号文をデータ部に含む暗号化ファイルを記憶部に書き込む。

【0104】暗号化ファイルの復号には、パスワードを用いる方法と鍵情報を用いる方法とがある。ファイル復号部300bは、鍵情報を用いる場合には、暗号化ファイルのヘッダ部から獲得した第2暗号化ファイル鍵を鍵情報を用いて復号し、ファイル鍵を求め、次に、暗号文をそのファイル鍵で復号する。パスワードを用いる場合には、利用者からパスワードの入力を受け付け、第1暗号化ファイル鍵をパスワードを用いて復号してファイル鍵を求め、次に暗号文をそのファイル鍵で復号してものの平文を求める。

【0105】2.4 変形例

ファイル管理装置10bは、次に示すように構成してもよい。

(1) パスワード登録部100bは、前記利用者IDの入力を受け付け、暗号化パスワードを、特定のコンピュータシステムの中で、利用者IDと対応させて保存しておいてもよい。このとき、ファイル暗号部200bは、さらに前記利用者IDの入力を受け付け、入力された前記利用者IDに対応付けられた前記暗号化パスワードを復号する。

【0106】(2) パスワードを変更する場合の動作について、図14に示すフローチャートを用いて説明する。パスワード登録部100bは、登録媒体20から鍵情報を読み出し、暗号化ファイル404bから第2暗号化ファイル鍵を読み出し、前記鍵情報を鍵として用いて第2暗号化ファイル鍵に復号アルゴリズムD4を施してファイル鍵を生成する(ステップS261)。次に、パスワード登録部100bは、新たなパスワードの入力を受け付け(ステップS262)、新たなパスワードを用いてファイル鍵に暗号アルゴリズムE2を施して新第1暗号化ファイル鍵を生成し(ステップS263)、次に、新第1暗号化ファイル鍵を暗号化ファイル404b内の第1暗号化ファイル鍵に上書きする(ステップS264)。

【0107】(3) パスワードによる暗号文の復号を禁止する場合には、ファイル管理装置10bは、暗号化ファイル404b内の第1暗号化ファイル鍵を削除する。このとき、鍵情報を用いた暗号文の復号は可能である。

(4) 鍵情報を変更する場合の動作について、図15に示すフローチャートを用いて説明する。

【0108】前記記憶媒体は、前記鍵情報(旧鍵情報と呼ぶ)に代えて、新たな鍵情報(新鍵情報と呼ぶ)を予め記憶している。ファイル暗号部200bは、前に入力されたもののものと同じパスワードの入力を受け付け

30

(ステップS281)、暗号化ファイル404bから第1暗号化ファイル鍵を読み出し(ステップS282)、前記パスワードを鍵として用いて、第1暗号化ファイル鍵に復号アルゴリズムD2を施してファイル鍵を生成する(ステップS283)。次に、ファイル暗号部200bは、記憶媒体から新鍵情報を読み出し、新鍵情報を鍵として用いてファイル鍵に暗号アルゴリズムE4を施して新第2暗号化ファイル鍵を生成し(ステップS284)、新第2暗号化ファイル鍵を暗号化ファイル404b内の第2暗号化ファイル鍵に上書きする(ステップS285)。

【0109】(5) 上記の実施の形態では、暗号化パスワードは、1個のコンピュータシステム内に保存しているので、パスワードによる暗号文の復号は、当該コンピュータシステム内でのみ可能となる。ここで、他のコンピュータシステムにおいて、パスワードによる復号を可能にするためには、暗号化パスワードを可搬型の記録媒体に格納し、他のコンピュータシステムに入力すればよい。

【0110】ここで、1個のコンピュータシステムのパスワード登録部は、SDメモ리카ードなどの可搬型の記録媒体に暗号化パスワードを書き込む。また、利用者は、暗号化ファイルを可搬型の記録媒体に書き込む。次に、利用者は、暗号化パスワードの書き込まれた記録媒体と、暗号化ファイルの書き込まれた記録媒体を他のコンピュータシステムに装填し、他のコンピュータシステムが輸入するファイル復号部は、可搬型記録媒体から暗号化パスワードを読み出し、復号し、また可搬型記録媒体から暗号文を読み出し、復号する。

【0111】ここで、暗号化パスワードと暗号文とを1個のファイルとして、1個の可搬型の記録媒体に書き込むとしてもよい。

(6) 平文を暗号化して暗号文を生成するときに、暗号化ファイルのヘッダ部に暗号化の有無や対応する鍵情報の利用者IDを格納し、鍵情報やパスワードが更新されたときに、上記(2)又は(4)の手順において、これら暗号化の有無や利用者IDなどの情報を用いて、暗号化ファイルを検索するようにしてもよい。また、各暗号化ファイルのヘッダ部にこれらの情報を書き込む代わりに、暗号化ファイル毎に、これらの情報を一括して一括ファイルに書き込んでおいて、一括ファイルを用いて、暗号化ファイルを検索するようにしてもよい。

【0112】(7) 平文を暗号化して暗号文を生成するときに、利用者からの指示を受け付けて、指示の内容によって、暗号化ファイルのヘッダ部に第1暗号化ファイル鍵を格納するか否かを選択するようにしてもよい。第1暗号化ファイル鍵を格納することが選択された場合には、上記と同様にして第1暗号化ファイル鍵を暗号化ファイルのヘッダ部に格納する。格納しないことが選択された場合には、第1暗号化ファイル鍵の生成と、第

(17)

特開2002-33727

31

32

1 暗号化ファイル鍵の格納とを行わない。第1暗号化ファイル鍵を格納する場合には、パスワードによる暗号文の復号が可能である。格納しない場合には、パスワードによる復号が禁止できる。

【0113】(8) 利用者が鍵情報を紛失した場合に、鍵情報による暗号文の復号を禁止するときに、ファイル管理装置10bは、第2暗号化ファイル鍵を削除する。これにより、紛失した鍵情報を不正者が入手して復号することを禁止でき、第2の実施の形態では、第1の実施の形態で不可能であった、鍵情報を紛失したときの当該鍵情報の一時無効化を可能にしている。このとき、パスワードを用いた暗号文の復号は可能である。

【0114】さらに、(4)に示す構成より、パスワードによる復号は可能である。こうして、新しい鍵情報が発行されるまで利用者本人は不自由なくファイルにアクセスできる。また新しい鍵情報が再発行された場合には、暗号化ファイルのヘッダ部を更新するだけで、新しい鍵情報を用いて、以降は復号できるようにできる。以下において、図16～図18に示すフローチャートを用いて、利用者が鍵記録媒体を紛失した場合の処理について、説明する。

【0115】これらのフローチャートに示すように、利用者が鍵記録媒体を紛失した場合には、鍵情報の一時無効化処理がなされる(ステップS301)。次に、鍵情報が一時無効化されている期間において、利用者が暗号文を復号するときには、パスワードによる復号処理がなされる(ステップS302)。次に、新鍵情報が発行され、新鍵情報を記録している鍵記録媒体が利用者に新たに提供された場合には、新第2暗号化ファイルを作成し(ステップS303)、新鍵情報を用いて通常の復号処理が行われる(ステップS304)。

【0116】次に、ステップS301～S304の詳細について説明する。ステップS301における鍵情報の一時無効化処理において、ファイル管理装置10bは、第2暗号化ファイル鍵を削除する(ステップS311)。ステップS302におけるパスワードによる復号処理において、パスワード入力部301bは、利用者からパスワードの入力を受け付け(ステップS321)、復号部302bは、記憶部400bから第1暗号化ファイル鍵を読み出し、前記パスワードを鍵として用いて、読み出した前記第1暗号化ファイル鍵に復号アルゴリズムD2を施してファイル鍵を生成し、前記ファイル鍵を切替部303bを介して復号部305bへ出力する(ステップS322)。次に、復号部305bは、記憶部400bから暗号化ファイル404bのデータ部に含まれる暗号文を読み出し、前記ファイル鍵を鍵として用いて、読み出した暗号文に復号アルゴリズムD3を施して復号文を生成し(ステップS323)、次に、復号部305bは、生成した前記復号文を含む復号文ファイル402bを記憶部400b内に書き込む(ステップS32

4)。

【0117】ステップS303における新第2暗号化ファイルを作成処理において、ファイル暗号部200bは、前に入力されたものと同じパスワードの入力を受け付け(ステップS331)、暗号化ファイル404bから第1暗号化ファイル鍵を読み出し(ステップS332)、前記パスワードを鍵として用いて、第1暗号化ファイル鍵に復号アルゴリズムD2を施してファイル鍵を生成する(ステップS333)。次に、ファイル暗号部200bは、鍵記録媒体から新鍵情報を読み出し、新鍵情報を鍵として用いてファイル鍵に暗号アルゴリズムE4を施して新第2暗号化ファイル鍵を生成し(ステップS334)、新第2暗号化ファイル鍵を暗号化ファイル404b内の第2暗号化ファイル鍵に上書きする(ステップS335)。

【0118】ステップS304における新鍵情報を用いる通常の復号処理において、復号部304bは、鍵記録媒体から新鍵情報を読み出し(ステップS341)、記憶部400bから新第2暗号化ファイル鍵を読み出し、前記新鍵情報を鍵として用いて、読み出した前記新第2暗号化ファイル鍵に復号アルゴリズムD4を施してファイル鍵を生成し、前記ファイル鍵を切替部303bを介して復号部305bへ出力する(ステップS342)。次に、復号部305bは、記憶部400bから暗号化ファイル404bのデータ部に含まれる暗号文を読み出し、前記ファイル鍵を鍵として用いて、読み出した暗号文に復号アルゴリズムD3を施して復号文を生成し(ステップS343)、次に、復号部305bは、生成した前記復号文を含む復号文ファイル402bを記憶部400b内に書き込む(ステップS344)。

【0119】(9) ファイル復号部300bは、暗号文の復号時に、鍵情報及びパスワードの両方を要求するようにしてもよい。また、第1及び第2暗号化ファイル鍵をそれぞれパスワード及び鍵情報を用いて復号して、2個のファイル鍵を生成し、生成された2個のファイル鍵が一致するか否かを判断することにより、暗号化ファイルのヘッダ部の改竄を検出するようにしてもよい。

【0120】(10) 第1の実施の形態の変形例と同様に、暗号化パスワード、第1暗号化ファイル鍵、第2暗号化ファイル鍵、暗号文に、認証情報を付加し、認証情報を用いて、これらの情報の改竄を検出するようにしてもよい。

3. まとめ

以上のように本発明によれば、計算機に付随した鍵情報を用いてファイルの暗号化と復号とが可能になる。加えて、暗号時に指定すれば復号時に鍵情報無しで、あらかじめ登録して計算機内に安全に保管しておいたパスワードを用いて復号が可能になる。ファイル暗号時には逐次パスワードを設定する必要はない。また、利用者がパスワードを忘却したときにパスワードによる復号を一時的

(18)

特開2002-33727

33

に無効化したり、新しいパスワードに容易に変更できる仕組みを備える。さらに、鍵情報を紛失したときに、鍵情報を一時的に無効化したり、新しい鍵情報が発行されたときにも、ヘッダ部だけを更新することにより、新しい鍵情報で前の鍵情報で暗号化したファイルを扱えるための仕組みを備える。また、鍵情報やパスワードのIDをヘッダや一括管理ファイルに格納することにより、鍵情報やパスワードの変更時にそれに伴う変更が可能である暗号化ファイルを検索することができる。

【0121】こうして、本発明では次の条件を満たすファイル暗号復号システムを提供することができる。

(1) ICカードのような記録媒体に格納した鍵情報を用いてファイルの暗号化を行なう。パスワードはあらかじめ登録しておき、逐一のパスワード入力は必要ないものとする。

【0122】(2) 前記鍵情報を用いてファイルの復号ができる。また、暗号化したときの指定によりあらかじめ登録したパスワードを用いたファイルの復号も可能とする。

(3) パスワードを容易に変更できる仕組みを備える。

(4) 前記鍵情報を紛失した場合に、一時的に鍵情報を無効化する仕組みを備える。さらに、新しい鍵情報が再発行された場合に、新しい鍵情報で以前のファイルが取り扱えるための仕組みを備える。また、そのために変更すべき暗号化ファイルを容易に検索する仕組みを備える。

【0123】4. その他の変形例

なお、本発明を上記の実施の形態に基づいて説明してきたが、本発明は、上記の実施の形態に限定されないのはもちろんである。以下のような場合も本発明に含まれる。

(1) 上記の実施の形態において、暗号及び復号アルゴリズムとしてDESを用いるとしているが、他の暗号及び復号アルゴリズムを用いてもよい。

【0124】(2) 本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フロッピー（登録商標）ディスク、ハードディスク、CD-ROM、MO、DVD、DVD-ROM、DVD-RAM、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。

【0125】また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク等を経由して伝送するものとしてもよい。また、本発

34

明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。

【0126】また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

(3) 上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

【0127】

【発明の効果】上記の目的を達成するために、本発明は、平文を暗号化して記憶し、復号するファイル管理装置であって、鍵情報を予め記憶している鍵記録媒体と、入力されるパスワードを用いて前記鍵情報を暗号化して暗号化鍵を生成する登録手段と、前記鍵記録媒体に記憶されている鍵情報に基づいて、平文を暗号化して暗号文を生成する暗号手段と、前記鍵記録媒体から鍵情報を読み出すか、又は入力されるパスワードを用いて前記暗号化鍵を復号して鍵情報を生成するかを切り換える切換手段と、前記鍵情報に基づいて暗号文を復号する復号手段とを備える。また、前記ファイル管理装置は、さらにメモリ部を有し、前記登録手段は、パスワードの入力を受け付け、前記パスワードを用いて前記鍵情報を暗号化して暗号化鍵を生成し、生成した前記暗号化鍵をメモリ部に書き込み、前記暗号手段は、ファイル鍵を用いて平文を暗号化して暗号文を生成し、前記鍵情報を用いて前記ファイル鍵を暗号化して暗号化ファイル鍵を生成し、前記暗号文と前記暗号化ファイル鍵とを対応付けてメモリ部に書き込み、前記切換手段は、前記パスワードの入力を受け付け、前記パスワードを用いて前記暗号化鍵を復号して鍵情報を生成する第1鍵獲得手段と、第2タイプの入力を受け付けた場合に、前記鍵記録媒体から鍵情報を読み出す第2鍵獲得手段とを含み、前記切換手段は、前記第1及び第2鍵獲得手段のいずれかにより鍵情報を獲得し、前記復号手段は、前記鍵情報を用いて前記暗号化ファイル鍵を復号してファイル鍵を生成し、前記ファイル鍵を用いて前記暗号文を復号して復号文を生成するように構成してもよい。

【0128】この構成によると、前記鍵記録媒体から鍵情報を読み出すか、又は入力されるパスワードを用いて前記暗号化鍵を復号して鍵情報を生成するかを切り換え、前記鍵情報に基づいて暗号文を復号するので、パスワードによらずとも復号することができる。また、本発明は、平文を暗号化して記憶し、復号するファイル管理装置であって、鍵情報を予め記憶している鍵記録媒体と、前記鍵情報を用いて入力されるパスワードを暗号化する登録手段と、ファイル鍵を用いて平文を暗号化して

(19)

特開2002-33727

35

暗号文を生成し、前記鍵情報と前記暗号化されたパスワードを復号して得られたパスワードとに基づいて、ファイル鍵を暗号化してそれぞれ暗号化ファイル鍵を生成する暗号手段と、前記鍵情報に基づいて暗号化ファイル鍵を復号するか、又は入力されたパスワードに基づいて暗号化ファイル鍵を復号するかを切り換えて、ファイル鍵を生成する切替手段と、前記ファイル鍵に基づいて暗号文を復号する復号手段とを備える。また、前記ファイル管理装置は、平文を暗号化してメモリ部に記憶し、前記登録手段は、パスワードの入力を受け付け、前記鍵情報を用いて前記パスワードを暗号化して暗号化パスワードを生成し、生成した前記暗号化パスワードをメモリ部に書き込み、前記暗号手段は、前記鍵情報を用いて前記暗号化パスワードを復号してパスワードを生成し、ファイル鍵を用いて平文を暗号化して暗号文を生成し、前記パスワードを用いて前記ファイル鍵を暗号化して第1暗号化ファイル鍵を生成し、前記鍵情報を用いて前記ファイル鍵を暗号化して第2暗号化ファイル鍵を生成し、前記暗号文と前記第1及び第2暗号化ファイル鍵とを対応付けてメモリ部に書き込み、前記切替手段は、前記パスワードの入力を受け付け、前記パスワードを用いて前記第1暗号化ファイル鍵を復号してファイル鍵を生成する第1鍵獲得手段と、前記鍵記録媒体に記憶されている鍵情報を用いて前記第2暗号化ファイル鍵を復号してファイル鍵を生成する第2鍵獲得手段とを含み、前記第1及び第2鍵獲得手段のいずれかによりファイル鍵を獲得し、前記復号手段は、前記ファイル鍵を用いて前記暗号文を復号して復号文を生成するように構成してもよい。

【0129】この構成によると、前記鍵情報に基づいて暗号化ファイル鍵を復号するか、又は入力されたパスワードに基づいて暗号化ファイル鍵を復号するかを切り換えて、ファイル鍵を生成し、前記ファイル鍵に基づいて暗号文を復号するので、パスワードによらずとも復号することができる。

【図面の簡単な説明】

【図1】第1の実施の形態としてのファイル管理装置10の外観を示す。

【図2】ファイル管理装置10の構成を示すブロック図である。

【図3】パスワード登録部100の動作を示すフローチャートである。

【図4】ファイル暗号部200の動作を示すフローチャートである。

【図5】ファイル復号部300の動作を示すフローチャートである。

【図6】利用者IDテーブルの一例を示す。

【図7】パスワードを変更する場合のファイル管理装置の動作を示すフローチャートである。

【図8】鍵情報を更新する場合のファイル管理装置の動作を示すフローチャートである。

36

【図9】暗号化ファイルのデータ構造の一例を示す。

【図10】第2の実施の形態としてのファイル管理装置10bの構成を示すブロック図である。

【図11】パスワード登録部100bの動作を示すフローチャートである。

【図12】ファイル暗号部200bの動作を示すフローチャートである。

【図13】ファイル復号部300bの動作を示すフローチャートである。

【図14】パスワードを変更する場合の動作を示すフローチャートである。

【図15】鍵情報を更新する場合の動作を示すフローチャートである。

【図16】鍵記録媒体を紛失した場合の動作を示すフローチャートである。図17へ続く。

【図17】鍵記録媒体を紛失した場合の動作を示すフローチャートである。図18へ続く。

【図18】鍵記録媒体を紛失した場合の動作を示すフローチャートである。図17から続く。

【符号の説明】

10 ファイル管理装置
10b ファイル管理装置
20 鍵記録媒体
100 パスワード登録部
100b パスワード登録部
101 パスワード入力部
101b パスワード入力部
102 暗号化部
102b 暗号化部
200 ファイル暗号部
200b ファイル暗号部
201 ファイル鍵生成部
201b ファイル鍵生成部
202 暗号化部
202b 暗号化部
203 暗号化部
203b 暗号化部
204b 暗号化部
205b 復号部
300 ファイル復号部
300b ファイル復号部
301 パスワード入力部
301b パスワード入力部
302 復号部
302b 復号部
303 切替部
303b 切替部
304 復号部
304b 復号部
305 復号部

(20)

特開2002-33727

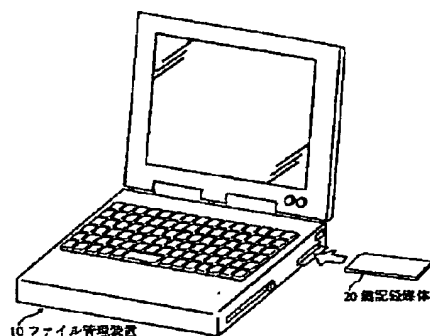
37

38

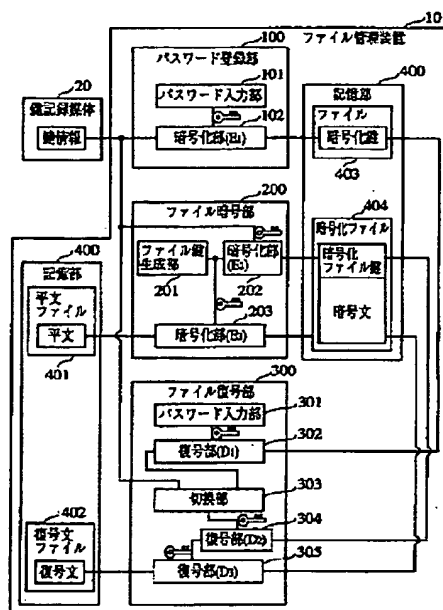
305b 復号部
400 記憶部

400b 記憶部

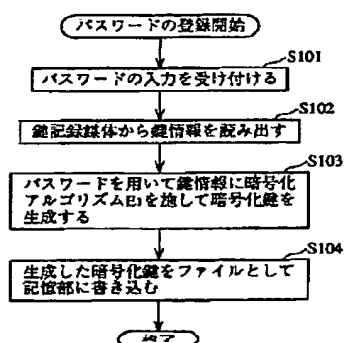
【図1】



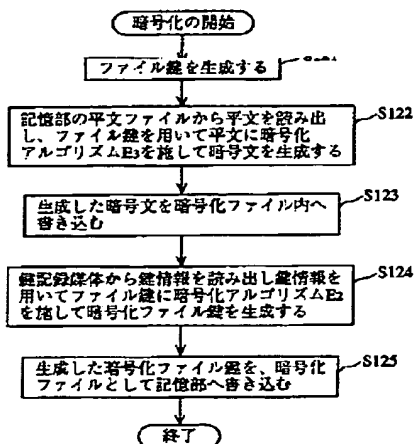
【図2】



【図3】



【図4】



【図6】

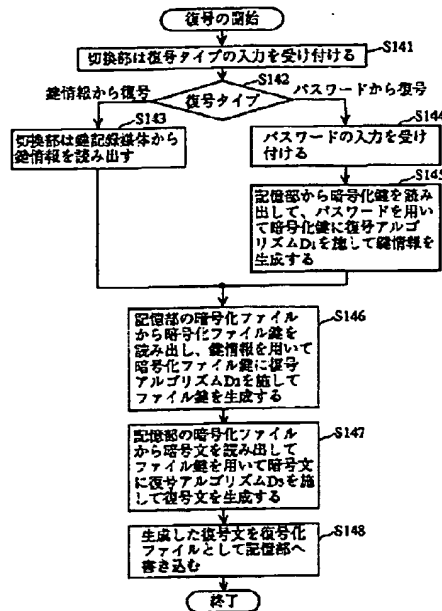
利用者IDテーブル

利用者ID	暗号化鍵
user 1	利用者1用暗号化鍵
user 2	利用者2用暗号化鍵
⋮	⋮

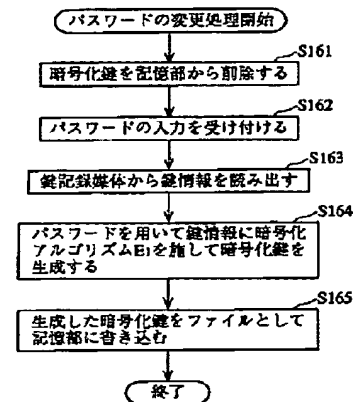
(21)

特開2002-33727

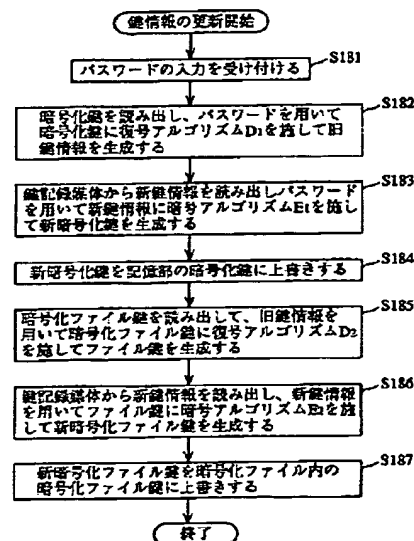
【図5】



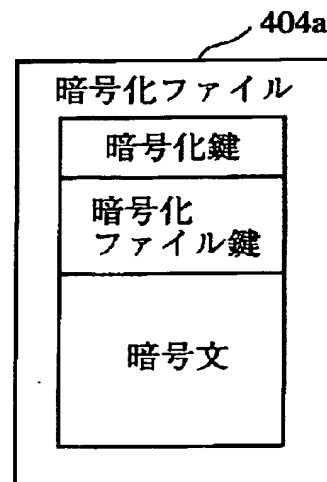
【図7】



【図8】



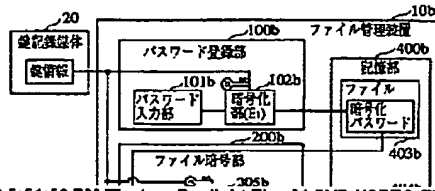
【図9】



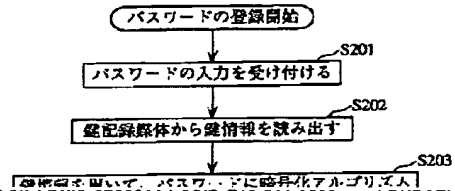
(22)

特開2002-33727

【図10】



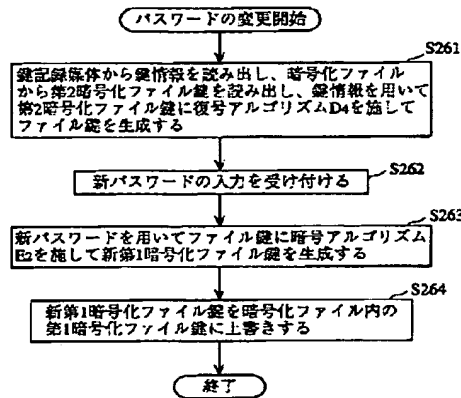
【図11】



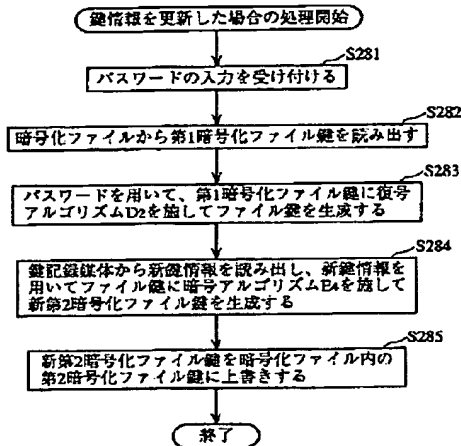
(23)

特開2002-33727

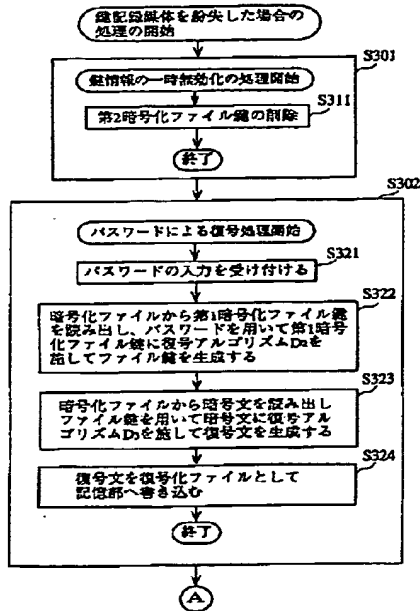
【図14】



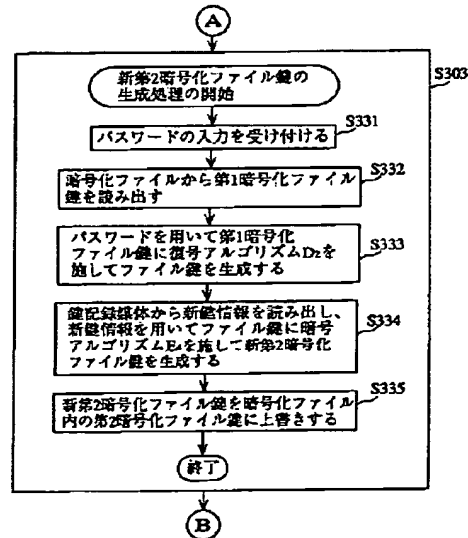
【図15】



【図16】



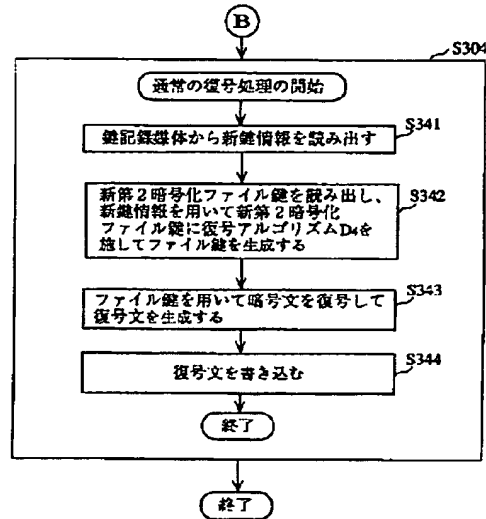
【図17】



(24)

特開2002-33727

【図18】



フロントページの続き

(51) Int. Cl. 7

H04L 9/32

識別記号

FI

H04L 9/00

7-73-D (参考)

601C

(72) 発明者 稲垣 恒

大阪府門真市大字門真1006番地 松下電器

産業 株式会社内

Fターム (参考)

5B017 AA03 BA07 CA16

5B082 EA11 GA11

5J104 AA16 EA03 EA04 EA11 EA26

JA13 NA02 NA05 NA12 NA35

NA37